UACES 45th Annual Conference

Bilbao, 7-9 September 2015

www.uaces.org

Artur Gruszczak
Associate Professor of International Relations
Jagiellonian University
Krakow, Poland
artur.gruszczak@uj.edu.pl

Building resilience: the role of EU intelligence community

Paper to the UACES 45th Annual Conference, Bilbao, 6-9 September 2015

Work in progress – do not quote without author's permission

Abstract

Resilience is an increasingly relevant feature of contemporary security policy. It is no longer a buzzword, it has turned in recent two decades to an analytical term useful in the study of continuity and adaptive change in objects and systems, including social and political systems. States and organizations have become increasingly aware of benefits drawn from the 'resilience dividend' for the sake of internal security, public order and systemic stability.

This paper is dedicated to resilience as an objective and a feature of the European Union as a security community. In this respect, resilience is conceived as the capacity of the EU as an international organization to prepare for disruptions and to build and reinforce capacity to achieve revitalization from past crises and failures. Since resilience is predetermined by situational awareness, preparedness, risk assessment and anticipation, intelligence is meant to become a core and indispensable form of organized activity of the state or a security community. Therefore, the emergence of an EU intelligence community should be identified with the growing need to enhance resilience and preparedness of the EU and its member states in the face of threats and dangers challenging security, stability and order within the Union. A thesis developed in this paper claims that the EU has been developing its joint intelligence capabilities with direct reference to resilience building and crisis management capabilities as principal mechanisms of security governance in the EU.

Keywords

resilience - anticipation – intelligence – security – European Union

Introduction

Resilience is an increasingly relevant feature of contemporary security policy. Deeply rooted in environmental sciences, it has proliferated across many fields of contemporary science. It has also been welcomed by practitioners and decision-makers as an agile formula of responding to varied challenges, dilemmas and contingencies. Built on systemic prerequisites, resilience has explored the issue of stability and sustainability of natural ecosystems focusing on factors and mechanisms ensuring adaptive capacity of ecosystems when disturbances, disruptions or crises emerge or occur.

In January 2013 Time magazine declared resilience the 'environmental buzzword' of 2013 (Walsh 2013). But resilience is no longer a buzzword, it has turned in recent two decades to an analytical term useful in the study of continuity and adaptive change in objects and systems, including social and political systems. As some authors say, it is now 'a perennial key word for our turbulent, unpredictable, transformative 21st century.' (Almedom, O'Byrne and Jerneck 2015, 9).

Resilience has also addressed in an appealing and stimulating way the problems of individual and organised safety, tackling such key issues as human security, public order, crisis management, national security strategies and policies, international security. States and organisations have become increasingly aware of benefits drawn from the 'resilience dividend' (Rodin 2014) for the sake of internal security, public order and systemic stability. Resilience permeated individual and group thinking about security in stressful circumstances and as such it drew growing attention of institutions and organizations in charge of safety management, crisis prevention and mitigation.

This paper is dedicated to resilience as an objective and a feature of the European Union as a security community. In this regard, resilience is conceived as a process of building and expanding the capacity of the EU as an international organization to prepare for disruptions and to achieve revitalisation from past crises and failures. Since resilience is predetermined by situational awareness, preparedness, risk assessment and anticipation, intelligence is meant to become a core and indispensable form of organized activity of the state or a security community. Therefore, the emergence of an EU intelligence community should be identified with the growing need to enhance resilience and preparedness of the EU and its member states in the face of threats and dangers challenging security, stability and order within the Union. A thesis developed in this paper claims that the EU has been developing its joint intelligence capabilities with direct reference to resilience building and crisis management capabilities as principal mechanisms of security governance in the EU.

Resilience – an essentially contested concept

Resilience has become for two decades a concept enjoying sympathy of practitioners (politicians, corporate managers, public decision-makers) (Brasset and Vaughan-Williams 2013) and raising a vast interest within the academic community. Many research projects have been conducted and a bulk of scholarly articles and papers have been published. Several interesting general and bibliometric papers convincingly document the growth of this academic industry (Janssen et al 2006; Janssen, Schoon, Ke and Börner 2006; Janssen 2007; Brand and Jax 2007; Walker and Cooper 2011; Grimm and Calabrese 2011; Xu and Marinova 2013; Brassett, Croft and Vaughan-Williams 2013; Brown 2014; Rogers 2015; Almedom, O'Byrne and Jerneck 2015; Dunn Cavelty, Kaufmann and Kristensen 2015). Resilience has become the phenomenon studied in many scientific areas and disciplines, such diverse as economics, mathematics, engineering, medicine, urban studies, environmental sciences, psychology, pedagogy, geography, management sciences, sociology, philosophy, security studies. The review of concepts made by de Van Breda (2001), Bruijne, Boin and van Eeten (2010), Walker and Cooper (2011), Kolar (2011) Brown (2014) and Schmidt (2015) provides extensively evidences on the variety and multiplicity of the meanings, approaches and perspectives.

In spite of the amassing scholarship, it has remained an essentially contested concept since it has been tested in the whole lot of cases ranging from ecological sustainability to political philosophy and more often causing a cognitive confusion due to the huge diversity of the concepts, meanings and definitions proliferating across different disciplines, theories and practices. Having originated in behavioral sciences, it was adopted and developed in the 1970s in theoretical and practical ecology, thanks to Crawford S. Holling's path-breaking article (Holling 1973), and in social sciences, owing to Friedrich August von Hayek's contribution to complex systems theory and the concept of the market as complex ecosystem (Walker and Cooper 2011, 148-149). Contemporary security studies adopted the concept of resilience quite belatedly. Thanks to Aaron Wildavsky (1988), the notion of resilience debuted in the vocabulary of safety sciences and then nested in such fields as, obviously, environmental security, and also risk management, safety engineering, policing studies, development studies and even critical security studies.

For the purposes of this paper, the conceptual framing of resilience is focused on some key elements of contemporary security as an institutionalised organisational practice performed in a very 'high-noise' environment. These elements are present in the definitional content of resilience including such cognate terms as: sustainability, adaptability, recovery, permanence, robustness, persistence, resistance, readiness, preparedness. These descriptors refer to resilience as a systemic property of structural security environment prone to fluctuations and changes over time. Departing from the classical Holling's and Wildavsky's definitions, resilience means the capacity of a system to cope with unanticipated dangers after they have become

manifest, to absorb change and disturbance and to learn to bounce back by reorganization and change ensuring the maintenance of essentially the same function, structure, identity, and feedbacks (Wildavsky 1988, 77, Holling 1973, 14; Walker, Holling et al 2004, 2; Edwards 2009, 18). Hence, resilience is pertinent to stability and robustness of a system, preparedness for unpredictabilities, unintended consequences and boomerang effects generated by dynamic, volatile and sometimes turbulent environment. As Lentzos and Rose highlight, resilience consists in 'a systematic, widespread, organizational, structural and personal strengthening of subjective and material arrangements so as to be better able to anticipate and tolerate disturbances in complex worlds without collapse, to withstand shocks, and to rebuild as necessary.' (Lentzos and Rose 2009, 243) Resilience can be seen as a process in which an entity – an individual, a community, an organisation - maintains basic functionalities when confronted with a serious disruption, outbreak or randomly emerging existential threat. It is conceived as a 'measure of a system's persistence and its ability to absorb change and disturbance but still maintain the same relationships among population or state variables' (Allen, Gunderson and Holling 2010, 5). So, resilience can be captured in a simplistic and radical wording as a special ability to react to traumatic or catastrophic events and its aftermaths 'as if nothing ever happened'.

Resilience can be conceptualised in two corresponding perspectives which can be merged in a cross-referential matrix. The first variable is the dynamic of security environment in which resilience is manifested. Here we can distinguish two forms: static and active. The former highlights stability as the key feature of a security system; the latter underlines the inherent unpredictability of system behavior. The second variable is the type of reaction to acute security problems in the temporal dimension. The emergence of a disruption, breakdown or disaster is the critical position in the timeline dividing the system dynamics in two main phases: pre-crisis prevention and post-crisis reaction.

Table 1. Variables of resilience

	Static	*Active*
Prevention	preparedness	anticipation
Reaction	recovery	transformation

The static form builds on the lexical meaning of resilience as 'the ability to bounce or spring back into shape, position, etc.' (Webster's 1986, 1210). Resilience depends on stability, balance, firmness. Alegorically, it can be depicted as a lonely house hit by terrible storm, resisting powerful hurricane wind and slanting rainfall, suffering certain damages and losses, but keeping its construction firm and unshaken, fulfilling thus successfully its essential function: protecting its inhabitants, ensuring they are safe and sound, safeguarding their material goods and resources. When the storm is over, some recovery is needed and repair mechanisms are put into action. So, the static approach is focused on stability rebalancing, recovery, bouncing back, return to 'normalcy'. The structural properties of security system in the pre-crisis conditions serve as a reference point and provide benchmarks for recovery action in the post-crisis circumstances.

The pre-crisis resilience refers to the capacity of awareness building in the face of potential and probable shocks and disruptions. It is associated with the management of surprise (Wildavsky 1988, 98). It is the ability to detect contingencies, identify random events and key risk factors (Kaplan 2002, 26-29) and enhance predictability in complex environment. This entails descriptive prediction and prescriptive planning on the basis of a deliberate framed-up strategy and commensurate scenarios articulating unknowns and uncertainties (Hukkinen, 2008: 102). The scenarios and plans explore the identified vulnerabilities of the system and calculate the related risks. Vulnerability, as Aradau and van Munster note, is a good risk indicator but is not completely adequate for analysing responses to sudden changes or catastrophic events. They underline that 'the goal of preparedness is not just to reduce vulnerability but to foster resilience.' (Aradau and van Munster 2011, 46). If we conceive of vulnerability as a predisposition to negative outcomes, susceptibility to persistent risks and unknowns, then we consider it a 'harbinger' of emergencies and disruptions which implies various forms of preparation and safeguarding. Preparedness must employ dedicated ways and means of handling the issue of systemic vulnerabilities by recurring to resilience as the property of dedicated security measures. It can be regarded as a set of instruments and techniques implemented by the government in the framework of security measures established to deal with emergencies and disasters (Neocleous 2013, 190). Preparedness is then the process of systemic capacity building in the pre-crisis phase with regard to defence against and resistance to the effects of a disruption or a crisis. It has to do with the management of available resources (material, financial, information, communication) in a way that ensures an enhanced ability to confront an immediate disruptive change or a sudden breakdown.

Recovery and reconstruction are another important aspects of the static form of resilience. Rodin, for instance, sees resilience as a component of crisis management cycle, highlights its importance in the post-disaster conditions. She conceives it as a capacity developed during emergencies or in crisis circumstances that could not have been avoided or prevented, a sort of lessons-learnt approach to

both future challenges and crises to come. She refers to the 'resilience dividend' as a value added to the general crisis management system enabling a quick and effective return to normalcy after a breakdown and fostering a systemic adjustment or even a 'significant transformation that yields benefits even when disruptions are not occurring.' (Rodin 2014, 12). So, she builds a link between the static and active responses to disruptions, crises or turmoils.

Rodin notes that sometimes bouncing back is not sufficient, the damage caused in the system is too big to reconstruct the previous setting and ensure its stability and proper performance (Rodin 2014, 12). This argument draws from Holling's obervation on stability as equilibrium. There has been a thread in resilience theory addressing the value of equilibrium for system stability and maintenance. Some authors conceived of bouncing back as 'the return of a system to an equilibrium state following disturbance' (Allen, Gunderson and Holling 2010, 5). In a similar vein, Grimm and Calabrese, who studied resilience of complex systems, asserted that resilience is one of stability properties of equilibrium-centred systems (Grimm and Calabrese 2011, 6). However, Holling in his original paper already noticed that 'an equilibrium centred view is essentially static and provides little insight into the transient behavior of systems that are not bear the equilibrium' (Holling 1973, 2, 15). We completely subscribe to Holling's reflection, especially as far as contemporary security systems are concerned. We also follow Walker and Cooper who claim that resilience is the 'acceptance of disequilibrium as a principle of organization' (Walker and Cooper 2011: 154).

Therefore, resilience embodies the transformative capability of the system exposed to sudden threats, pressures and tensions so as to prevent an emergency or disruption, avoid a looming crisis and keep security mechanisms running properly. The transformative power is even more important in the post-crisis phase. It entails a good deal of measures and means aiming to adjust the system to new conditions and factors determining the overall performance of security mechanisms and procedures. It corresponds with the past experiences and lessons learnt but it also looks forward to handling present dangers and cope with problems to come. Resilience then means the capacity of 'being able to come away from the event with an even greater capacity to prevent and contain future errors' (Weick, Sutcliffe, and Obstfeld 2002, 14 quoted in de Bruijne, Boin and van Eeten 2010, 23). It also consists in stimulating positive feedbacks within the complex security system and increasing protective skills of its institutional components.

Another aspect of the active form of resilience refers to prevention of catastrophic events and disruptive changes through the use of anticipatory techniques and early warning mechanisms. Planning and foresight have always been considered relevant factors enhancing resilience as a preventative measure. The fear of a fundamental unanticipated surprise has represented a major challenge to resilience (Wears and Webb 2014, 42). An active approach to this challenging issue requires the application of anticipatory measures. Pre-cautionary and forward-looking

tools and techniques aim to build up a picture or a scenario of future developments. Awareness of dysfunctional elements of security systems stimulates proactive maintenance and disaster mitigation. So the wish to confront the threats before they materialise and turn to present dangers or disruptive changes has been the essence of anticipatory approaches and measures.

Aaron Wildavsky opposed anticipation to resilience. He conceived anticipation as a kind of efforts made 'to predict and prevent potential dangers before damage is done.' Resilience instead is meant as 'the capacity to cope with unanticipated dangers after they have become manifest' (Wildavsky 1988, 77). He added that anticipation seeks to avoid hypothesized hazards and concluded that both anticipation and resilience are well suited to different conditions. Anticipation makes sense under substantial certainty and predictability (Wildavsky 1988, 79-80). Using a vocabulary popularised fifteen years after (Rumsfeld 2011; 2013), anticipation is about 'known unknowns' while resilience is about 'unknown unknowns'. Both require a full situational assessment of endogenous and exogenous variables and analytical insights into the structure and dynamics of the security environment.

Holling pointed out that the behavior of ecological system – and one can extend this remark on social and security systems – was 'profoundly affected by random events.' (Holling 1973, 13). The latter disclaimer is correct but it does not mean that resilience is tested in totally unpredictable circumstances and realized only post factum. As we have already noted, preparedness and anticipation are two facets of the preventative form of resilience. They start from the assumption that the future is predictable and that some advanced security systems are able to calculate through a wide range of tools and techniques the probability that a threat, a disruption or a catastrophe will occur (Anderson 2010, 783-784).

The real challenge for these systems is the increasing complexity and uncontrollability of security area. The more complex system, the harder it is to anticipate its outcomes. Comfort and others rightly underlined the consequences of increasing complexity for the organisational performance of public and private organisations. They stressed that: 'Increases in organized complexity require significant increases in information flow, communication, and coordination in order to integrate multiple levels of operation and diverse requirements for decision into a coherent program of action.' (Comfort et al 2001, 144). Therefore, anticipation should enhance the abilities to detect, monitor, respond and learn. Hollnagel wrote: 'Learning can be used to improve the ability to respond, to select appropriate indicators and cues and also to hone the imagination that provides the basis of anticipation. Monitoring can primarily be used to improve the ability to respond (increased readiness, preventive responses). And responding can provide the experience that is necessary to improve learning as well as anticipation.' (Hollnagel 2014, 189).

The above described matrix of 'resilience in action' presents a heuristic viewpoint that resilience writ large cannot be confined to the capacity to cope with

unanticipated occurrences which might bring about negative consequences for stability and performance of an entity. In our perspective, resilience entails inevitability of systemic disruptions or outbreaks due to imperfect organisational networks, ineffective communication channels and distorted information flow. However, resilience implies a dynamic approach to dysfunctional and crisis-prone elements of the environment. It highlights the importance of adaptability and constructive recovery as well as anticipatory skills and preventative abilities acquired through the extensive use of knowledge management, information analysis and learning.

Resilience and intelligence – an intimate relationship

The general concept of resilience alludes to information, knowledge and awareness as structural elements of the security environment. Wildavsky wrote about general resources, such as knowledge, education, wealth, energy, communication (Wildavsky, 1988, 13). We will focus on information, knowledge and intelligence as the most important among 'general resources', considering them as 'strategic resources' indispensable for resilience building in the contemporary complex networked security environment.

Evans and Reid (2013: 95) remark that: 'What resilience preaches is the impossibility and folly of even thinking we might resist danger and, instead, accept the necessity of living a life of permanent exposure to endemic dangers'. Contrary to this assumption, we claim that the permanent exposure to perils, risks, and hazards, inevitable and 'natural' in a sense, does not limit resistance capabilities and chances for an effective defence and constructive reaction in the face of a danger, a disruption or a collapse. Intelligence, conceived as the use of information and knowledge for analysis and assessment of the existing vital problems with the aim of helping to manage or solve them, is an activity which contributes to resilience building and maintenance. Resilience entails predictive abilities and so does intelligence. Resilience requires a clear picture of the complex environment; intelligence is focused on providing necessary information, knowledge and analysis used for a comprehensive assessment of a given aspect of the reality. Resilience addresses the issue of systemic vulnerabilities at the stage of preparedness; intelligence seeks to reduce long-term vulnerabilities in a strategic perspective. Resilience is juxtaposed with anticipation as two opposing features of dynamic uncertain environment, 'two strategic alternatives for securing safety (...).' (Wildavsky 1988, 8). Intelligence has decisively shifted towards anticipation and strategic forecast; resilience corresponds to anticipation as a complementary capacity enabling a better identification and assessment of risks and threats. The value of

intelligence is in its predictive capacity, anticipatory power and early warning capability that facilitates policy planning, strategic assessment and proper understanding of developments and trends in the future.

Evans and Reid (2013, 91-92) note that one of the effects of resilience is the importance of shared knowledge and information in responding to the logic of development of living systems determined by constant exposure to threats and systemic shocks. Hence, to be resilient means to know what are the critical variables and key parameters of the security ecosystem and to know how to detect, identify and evaluate factors undermining potentially or effectively the stability and efficiency of the system. Resilient systems must rely on systematic, reliable and effective means and modes of information management and knowledge sharing. This kind of activities can be realized in a certain institutional setting and must involve specialised agencies with clear-cut competences, specific skills and proper tools. This requirement in the case of complex security systems can be met only be an organised, efficient and cohesive set of intelligence services responsible for managing the vast area of communication and information available from open, secret and sensitive sources. Such an institutional arrangement may be called intelligence community if it serves the shared strategic objectives, ensures interconnectivity of its elements and enables a constant and smooth information and intelligence workflow.

It is a commonly shared argument that intelligence as an institution and also as a process of information management emerged in response to natural existential anxieties (Wheaton and Beerbower 2006, 329). Fear, uncertainty, distrust, unpredictability have accompanied the nation-, state- and community-builiding processes. As one of intelligence scholars observed, 'The purpose of intelligence since time immemorial has been to reduce uncertainty about the aspirations, intentions, capabilities, and actions of adversaries, political rivals, and, sometimes, partners and allies.' (Fingar 2011, 6) Intelligence, according to Manosevitz (2013, 15), helps policymakers to avoid surprise, understand evolving situation, as well as identify opportunities to advance national objectives or avoid risks to vital security interests. It is then corresponding to resilience objectives in terms of preparedness, situational awareness or contingency planning. Also, it takes up the issue of alerting and early warning as methods activating resilient elements of the security system. In strategic terms, intelligence prepares long-term assessments and situation trends but also provides warning of immediate threats to vital security interests (Johnson and Wirtz 2004, 2). Some scholars claim that 'Intelligence is more about early warning, strategic foresight, and real-time decision support for cooperative risk management than about gaining a secret advantage over a single state adversary.' (Sullivan 2007, 17). It may entail global and sectoral situational estimates, threat assessments and risk analyses. But it also has to develop alerting and threat warning in order to launch crisis management activities in early-warning stage. Foreseeing and alerting discontinuities in preparedness and resilience are of utmost importance for the general performance of the complex security system (Grabo 2002; Waltz 2003).

Sometimes intelligence brings forth a 'self-fulfilling prophecy', i.e. contributing to resilience building through information analysis and intelligence production, it may also raise awareness of potential enemies or hostile actors and encourage them to look for weak points or shortcomings of the security system. Paradoxically, 'resilience fosters an exposure to the catastrophic' (Evans and Reid 2014, 48). Intelligence, then, has to strive to discern actions or developments that were not anticipated or put on an indicator list, which 'in fact may be unique to the particular situation and might not occur another time.' (Grabo 2002, 27). Following Julian Richards we can point at a very important feature of intelligence as an ingredient of resilience, i.e. its forward-looking and predictive capacities. Organising intelligence around these functions is hard and demanding because it consists in the 'use of analysis of fragmented information and modelling of past activities and behaviours to predict what might happen in the future.' (2010, 23). It has to do with the learning aspect of resilience, i.e. the ability to draw lessons and innovate. Knowledge management and learning processes should ensure that intelligence is focused on relevant threats and risks and can effectively frame strategic policies, priorities and resource, thus giving key support to resilience (Akhgar, Yates and Lockley 2013, 6). Predictive capacities reduce the level of uncertainty and facilitate resilience building in its preparatory phase.

The immense proliferation of intelligence methods, means and tools across different layers of contemporary complex security systems has shown the growing importance of information gathering, processing and analysing, especially with reference to vital security interests of the states and their societies. For an effective resilience, it has been evident that the growing interconnectivity of information sources may bring about both positive and negative outcomes. However, it is taken for granted that such a situation stimulates various forms of cooperation in collecting, processing and sharing available information and data.

Contemporary security systems must cope adequately with complexity, diversity and wide range of activities undertaken by countless participants of public life. Accurate intelligence is essential for an effective and legitimate security management and is equally important for organisational performance. This rule is binding on both the state and an international organisation.

The EU intelligence community as a resilience provider

Current security challenges for the European Union as an international organisation and as a community of its member states require a consistent, pro-active, intelligence-led response. This politically motivated objective has to be shared by EU institutions and agencies and should engage the member states into a more intense

cooperation. Hence, data exchange, intelligence sharing and intelligence-led operations make up a specific security *zeitgeist* which inspires national and supranational counterparts to make stronger efforts and invest their resources to the making of a strategic intelligence community within the EU. Recent developments have just proved the well-known principle of knowledge dominance in the realm of security and made the public aware of the size, scope and depth of state policies in this regard. The EU is no exception and it has shown that the proposals and initiatives undertaken in recent years were timely and adequate to the emerging problems of information analysis, knowledge management and intelligence sharing. The proliferation of threats to security demands a functional intelligence architecture. The European Union has responded to this challenge gradually developing connections and linkages between relevant authorities of the member states and carefully yet systematically engaging available EU agencies and bodies in intelligence-led cooperation.

At the end of the 1990s EU member states along with relevant EU institutions and units started the building of an intelligence community on the basis of effective rendering of time-sensitive intelligence, development of estimation and analysis capabilities and sharing of best practices and analytical products. This decision was caused by the consequences of the evolution of post-Cold War global security environment, in particular the proliferation of transnational and cross-border threats increasingly affecting the integration process within the EU. The creation of the Schengen free-travel area obliged the member states to put more emphasis on cross-border cooperation in preventing and fighting crime as well as reinforcing their frontiers and modernise border infrastructure. Information and data exchanged between police officers, border guards and intelligence services of the member states was growing in numbers and relevance, overcoming thereby some member states' reservations and reluctance to a further cooperation in intelligence field. Moreover, EU heads of state or government in a follow-up to several bi- and multilateral summit meetings in the late 1990s and early 2000s highlighted the need to develop intelligence collection and analysis capabilities as a necessary component of the European Security and Defence Policy (ESDP) (Villadsen 2000).

These requirements were evident in the traumatic year 2003 when the EU, despite 'transatlantic rift' over US-led military invasion on Iraq, managed to launch its first military missions (in Macedonia and DR Congo), to make arrangements with NATO under the Berlin Plus agreement and articulate its global outlook in a single document - the European Security Strategy (ESS). The latter heralded an ambitious project of assuming by the EU a new global role in waging active policies to counter the new dynamic threats.

The events of 11 September 2001 highlighted the critical importance of intelligence for effective prevention and combating of terrorism and transnational crime. Efforts aimed to encourage a more intense and effective exchange of criminal information and intelligence did not, however, yield the expected results, mostly due

to the lack of unanimity and the deficit of trust among the member states. In the immediate aftermaths of the 11 March 2004 terrorist attack in Madrid, EU institutions placed particular emphasis on the exchange of information and intelligence between law enforcement authorities of the member states and called for the improvement of mechanisms for cooperation and the promotion of effective systematic collaboration between police, security and intelligence services (Friedrichs 2008; Deflem 2010; Argomaniz 2011).

Having reviewed thoroughly the obstacles to an effective exchange of information between law enforcement authorities in member states, the European Commission in 2004 concluded that they can only be effectively addressed on the basis of a firm commitment of member states to set up a European Criminal Intelligence Model (ECIM). This model comprised a common methodology of a reliable threat assessment. It rendered intelligence-led law enforcement effective and allowed for enhanced cooperation in the field of prevention and fight against terrorism and other forms of organised crime (Brady 2008; Kaunert 2010; Gruszczak 2013). The concept of the European criminal intelligence took shape of an intelligence cycle which relied on inputs from Europol and the member states contributing either directly or through appropriate institutional or working schemes as provided in EU law.

The concept of ECIM was taken into consideration in the EU Internal Security Strategy (EU ISS) adopted in early 2010 to further improve security in the EU, protect safety of citizens of the Union and tackle organised crime, terrorism and other threats. The strategy highlighted prevention and anticipation as mechanisms aimed to detect future threats and prevent their happening. It called member states to foster information exchange on a basis of mutual trust and share intelligence in time in compliance with the principle of information availability.

The EU Internal Security Strategy provided a strategic framework and broad guidelines for a comprehensive approach to effective intelligence-led policing and enhanced criminal intelligence cooperation among EU member states with a direct and active involvement of competent EU agencies and bodies (Gruszczak 2013). It laid solid grounds for criminal intelligence conceived as a critical element of evidence-based cooperation in the area of internal security in the EU, supported by the best available assessments and risk analyses, and overwhelmingly accepted patterns of resilience (Kaunert 2010).

A comprehensive response to the challenges of resilience building and security governance in the EU called for the making of a genuine EU intelligence community on the basis of scattered institutional and functional arrangements. Due to the existing legal, institutional and strategic divisions, the EU intelligence community had to adjust to a network configuration of security interests of EU member states expressed at the national level as well as through relevant EU institutions and bodies. The objectives and missions realized in the framework of the Common Security and Defence Policy (CSDP) retained their specific character, especially in the field of

information gathering and analysis as well as intelligence sharing. Military intelligence in the EU has been directly and thoroughly bound up with the CSDP. Therefore, it has reflected specific strategic, organisational, functional and political prerequisites which are deeply nested in ideological construction of EU identity (Kølvraa 2010) and the formation of the EU's actorness in international and global dimensions.

Intelligence capacities for the purposes of EU CSDP have been largely dependent on the member states. Although the value and importance of open source information gradually increased, defence intelligence organisations from EU member states have had the pivotal role in determining the real input and workflow of information and intelligence within the EU CSDP. CSDP missions and operations also involved crisis management and early warning, mostly due to the 'expeditionary' dimension of EU crisis management capabilities. Some elements of early warning and crisis prevention can be also found in the EU's common foreign policy and external relations as well as in internal security cooperation. Socio-cultural intelligence adopted in support of the EU's diplomacy and external relations consisted in collecting and analysing a plenty of data and information referring to crises, emergencies and hazards occurring outside the European Union yet having considerable, often serious or negative, impact on EU policy, identity or security. Exogenous threats like terrorism, organised crime, illegal migration or cyber attacks had to be anticipated and possibly prevented from occurring. EU internal security cooperation, though focused on criminal intelligence analysis, entailed also elements of situational intelligence acquired from early warning systems and strategic assessment mechanisms.

The mosaic of security fields in the EU determined the institutional setting and functional arrangements of EU intelligence community. Military intelligence has been concentrated in the EU Military Staff (EUMS). Its Intelligence Directorate relies principally on classified contributions from military intelligence services of the member states. The provision of information and analytical materials is limited and confined to need-to-know procedures. Strategic intelligence production in the EUMS is supported by the all-source analysis for the purposes of situational awareness, threat assessment and anticipatory capacity of policy-making. The Intelligence Directorate receives information from all CSDP crisis management missions, including data identified and recorded personally by officials participating in a given mission. It is also fed by other EU agencies, namely the EU Satellite Centre (SatCen) and the EU Intelligence Analysis Centre (IntCen), which provide the EUMS with geospatial intelligence (SatCen) and analytical products prepared on the basis of inputs provided by national civilian intelligence services (IntCen).

Visual observation and surveillance, as well as geospatial analysis of physical features and geographically referenced activities in the area of military operations and crisis management became widely implemented as a result of technological advancement and wider access to geospatial data (Darnis and Veclani 2011, 5-9).

The EU Intelligence Analysis Centre (IntCen) is a unit active in the field of CSDP but it also deals with problems of internal security, like trafficking of arms or terrorism (House of Lords 2003; Bigo et al 2007). It is a kind of facilitator for civilian intelligence services with regard to the exchange of security-related processed information (Davis Cross 2013). It works on open source material, military (thanks to cooperation with the EUMS) and non-military intelligence as well as diplomatic reporting. It has focused on the matters related to the CSDP, crisis management missions, forthcoming military and civilian operations, and immediate reactions to new threats which should be tackled by the mixture of military and civilian instruments (Müller-Wille 2008).

The Crisis Response System (CRS) established within the European External Action Service (EEAS) deals with emerging or enduring crises and supports the political decision making with regard to a given crisis situation. The CRS is tasked with an effective implementation of standard procedures in the context of the EU's ability to tackle crises and tensions taking place outside the EU or generated inside the Union by external drivers, which may affect EU security interests. Information sharing is one of the priorities of the Crisis Response System. Two components of the CRS are particularly engaged in information management and sharing among the member states and relevant EU institutions and bodies. They are the EU Situation Room (SitRoom) and the Crisis Platform. The Situation Room is responsible for channelling, selecting, collating and verifying all-source information available on crisis situations (Miozzo 2014). It is the only 24/7 capability at the EU level acting as a permanent switchboard for the EEAS and the European Commission, enabling the delivery of accurate and up-to-date crisis-related information to the decision makers. It draws information from all available sources, including open sources, EU delegations, Member States, EU CSDP Operations and Missions, EU Special Representatives' teams, EEAS exploratory missions, and relevant international organisations (Nimark and Pawlak 2014; High Representative 2011).

The EU Crisis Platform is an ad hoc undertaking activated and chaired by the High Representative of the Union for the Foreign Affairs and Security Policy / Vice-President of the European Commission (HR/VP) within the institutional framework of the EEAS and connected with relevant Commission services and General Secretariat of the Council. It aims to provide adequate and timely response to external crises requiring a coordinated action at the EU level. It seeks to facilitate information-sharing amongst participants during all phases of an ongoing crisis. The Crisis Platform collects, processes and disseminates to participants information and analyses relating to the most relevant aspects of a given crisis situation, including political issues, economic situation, social relations, military issues, humanitarian concerns and international environment. It enables EU officials and national experts invited to the Platform to get access to well-ordered and streamlined knowledge and also to keep information circulating among different institutional stakeholders.

Military and civilian intelligence sectors within the EEAS meet within the format of the Single Intelligence Analysis Capacity (SIAC). The SIAC was established with the aim of pooling civilian intelligence obtained by the IntCen with intelligence provided by the EUMS with regard to early warning and situation assessment (Jones 2012, 3; van Buuren 2009, 10; Norheim-Martinsen 2013, 98). The SIAC is collating, processing and analysing inputs coming from various sources: military and civilian Intelligence services of the member states, diplomatic missions of the EU (EU Special Representatives, Commission representations), ESDP Missions and international organisations, like the UN or the OSCE. Moreover, the SIAC can be fed by dedicated EU agencies, like SatCen, and can draw information from open sources. This cooperation allows the both the EUMS and the IntCen to operate jointly and to combine their analysis tools, generating a wide range of intelligence products from different sources (Haag and Anaya 2011, 8; Kozłowski and Palacios-Coronel 2014, 10).

EU internal security policy is founded on an intelligence-led policing model. It represents a pro-active approach to threat assessment and risk management on the part of relevant EU agencies and the majority of the member states, reflecting the growing importance of prevention and anticipation in the field of EU internal security. Intelligence-driven co-operation among national police and other law enforcement agencies became a showcase of modern transnational policing in the EU. The model of intelligence-led policing at EU level is grounded on specific functional and institutional synergies suitable to EU legal and institutional framework as well as national interests and perspectives of the member states.

The underlying function of intelligence-led policing is to anticipate crime trends and proactively create effective prevention strategies (Guidetti and Martinelli 2009). It may be also conceived as a 'type of law enforcement in which resources are deployed based on information gathered and analyzed from criminal intelligence.' (White 2009, 423). Intelligence-led policing therefore should be seen as a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving (Peterson 2005; Ratcliffe 2008), which is particularly suitable to the multi-level architecture of EU cooperation in police and criminal justice.

Europol is an EU agency endowed with enhanced capabilities in the area of information management, intelligence production and sharing, as well as operational support for the Member States. Europol has been tasked to lead the further development of the European Criminal Intelligence Model (ECIM). In this regard, it has develop a common EU approach for targeted collection and sharing of key criminal information, integrated analysis of financial intelligence linked to all crime phenomena, identification of top criminal targets. It also improved and strengthened the methodology of organised crime threat assessment (OCTA) being a part of the EU policy cycle for organised and serious international crime, established in 2010 on the basis of the intelligence-led policing approach.

Europol was designated as the 'central EU capability to receive, store and analyse this collected information' and to support operational activities of the Member States based on Europol's earlier strategic assessments. Europol has been equipped with enhanced capabilities in the area of information management, intelligence production and sharing. It delivers regular threat assessments and situation estimates with regard to terrorism and organised crime (Bures 2011, 96; Deflem 2006; Deflem 2010).

EU internal security has often been focused on the peripheral areas, territories bordering with third countries and separated by external borders of EU member states. The EU established in 2005 Frontex agency for the management of operational cooperation at the external borders of the member states (Neal 2009). The extensive field of Frontex's competences includes collection and analysis of information concerning the situation at the external borders and distribution of tailor-made intelligence products to relevant customers with the aim of providing as complete picture as possible of external risks and threats, building situational awareness and predicting future trends.

Frontex has used several analytical tools for risk analysis and situational intelligence at the external borders. Amongst them, the most important is the Common Integrated Risk Analysis Model (CIRAM). Initially, it was based on a six-field matrix, bringing together elements of criminal intelligence and risk assessment (Carrera 2007, 15-16). CIRAM was updated in 2011 in order to better respond to the changing external environment of the EU, to deal effectively with new types of risks and threats and to reflect the legal changes, both of which emphasised risk analysis as a key tool in ensuring the optimal allocation of resources and efficiency of equipment (Frontex 2013a, 11). Most importantly, Frontex is authorised to collect and process personal data of individuals who are subject to operational activities conducted or commanded by Frontex, like joint return operations, pilot projects and rapid interventions at the external borders. Collated information, including personal data, is further processed for strategic and operational purposes as well as a contribution to the analytical and operational work of other EU law enforcement agencies, mainly Europol.

Currently CIRAM is characterised by a management approach to risk analysis that defines risk as a function of the threat, vulnerability and impact (Frontex 2013a, 11). It is utilised for strategic and operational purposes. Concerning the latter, it supports the coordination of joint operations at the external borders conducted or coordinated by Frontex. It provides a background for an overall assessment of conditions, determinants and circumstances existing in the area of a planned joint operation at EU external borders. This picture is a sort of security landscape and is drawn on the basis of vast data flow containing various detailed information delivered by operational personnel made available by the Member States as well as acquired from public sources. This type of analysis is focused on identifying areas and sources of elevated risk or imminent threats and deciphering migratory routes,

the main nationalities or countries of origin of migrants as well as modi operandi of criminal groups or smuggling networks operating in the area of Frontex's planned activities.

To be effective and reliable in its analytical properties, CIRAM relies on a four-tier access control model that involves gathering information from numerous sources dispersed over the territory of EU member states. To this end, the Frontex Risk Analysis Network (FRAN) was established in 2007. It provides the framework for sharing knowledge and producing analytical and strategic reports on the current state of play at the external borders linking the intelligence networks of individual countries with Frontex (Frontex 2013b). The cooperative framework of the FRAN and its subsidiary, the European Union Document-Fraud Risk Analysis Network (EDF-RAN), feeds Frontex Risk Analysis Unit (RAU) with data which are processed, analysed and disseminated in form of analytical products. The most important are quarterlies, semi-annual and annual risk analyses. Moreover, RAU issues occasional documents and other tailored risk-analysis products.

Risk analysis model implemented by Frontex reflects pro-active approach to public order and internal security of the EU. It is mostly dealing with the problem of increasing criminality at EU external borders, taking form of transnational organized criminal networks involved in trafficking in human beings (Seiffarth 2011). This is why Frontex's methodology combines quantitative risk analysis, which relies on mathematical models and techniques to identify, quantify and manage exposures, with qualitative risk management, which focuses primarily on experience, judgment and common sense. However, the prevalence of quantitative data in Frontex's analytical tradecraft suggests that the agency is focused on 'hard' border security issues that could underpin cost-benefit approach to EU immigration and asylum policies. In this respect, selective differentiation at the external borders seeks to facilitate information management and enhance risk analysis capabilities of Frontex as well as national risk assessment units in the Member States.

Conclusions

The EU's experience in the building of intelligence community has proven the increasing significance of information management and intelligence sharing for resilience of the EU as a complex security system. Resilience entails the growing preventive capacities, anticipatory techniques and contingency measures; all require firm, substantial and continuous access to knowledge and information of critical security problems. The EU has been trying to acquire an added value linking tremendous amount of information sources located in the member states and building synergetic connections and functional interactions among variegated stakeholders.

Boin, Ekengren and Rhinard (2014) identified a wide array of EU institutional settings and working arrangements comprising 84 systems and tools dedicated to gathering, analysing and sharing information only in the area of crisis management. Even if only a few of them deal with full-fledged intelligence, the impressive number and variety of EU 'sense-making' arrangements underscore their relevance for early warning, crisis management, threat prevention and, finally, resilience building.

Intelligence cooperation developed recently in the EU has been characterised by the progressive adaptation and implementation of qualitative and quantitative methods of data analysis and information management by competent EU agencies and units, most of all Europol, Frontex, IntCen and SatCen. This trend corresponds with the reinforcement of the active pre-crisis approach focused on anticipation, early detection and warning of potential and substantial threats and disruptions. The EU as the security intelligence community took responsibility for establishing, developing and improving coordination between its relevant agencies and entities and the national intelligence services of the member states active in both civil and military fields. As a result, it has got access to the plenty of information sources and developed all range of mechanisms and tools enabling an efficient gathering and analysing of data and information referring to threats, risks and security concerns. This is a huge potential for building resilience of the EU security system on the basis of accurate, reliable and timely strategic security awareness connected with early-warning mechanisms and crisis response schemes.

The EU intelligence community is still decentralised and relied on varied cooperative networks. As such, it is subject to national predilections and habits which quite often restrict the scope of involvement in intelligence cooperation at EU level. The challenge of integration, cross-referencing and checking of all available information material must be met at the political level, demanding from EU top officials and representatives of the member states a more open and flexible attitude to information sharing and intelligence production.

References:

Akhgar B, Yates S and Lockley E (2013) 'Introduction: Strategy Formation in a Globalized and Networked Age - A Review of the Concept and its Definition.' In Akhgar B and Yates S (eds), *Strategic Intelligence Management. National Security Imperatives and Information and Communications Technologies* (Waltham, MA and Kidlington: Butterworth-Heinemann), 1-8.

Allen C R, Gunderson L H and Holling C S (2010) 'Commentary on Part One Articles.' In Gunderson L H, Allen C R and Holling C S (eds) *Foundations of Ecological Resilience* (Washington - Covelo - London: Island Press), 3-18.

Almedom A M, O'Byrne D and Jerneck, A (2015) 'Principles of epistemological accountability with methodological implications for measuring, assessing, and profiling human resilience.' *Ecology and Society* 20 (3), 9.

Anderson B (2010) 'Preemption, precaution, preparedness: Anticipatory action and future geographies.' *Progress in Human Geography* 34 (6), 777–798.

Aradau C and van Munster R (2011) *Politics of catastrophe: genealogies of the unknown* (London – New York: Routledge).

Argomaniz J (2011) *The EU and Counter-Terrorism. Politics, polity and policies after 9/11* (London and New York: Routledge).

Bigo D et al (2007) 'Mapping the Field of the EU Internal Security Agencies.' In Bigo D (ed) *The field of EU Internal Security Agencies* (Paris: L'Harmattan / Centre d'Etudes sur les Conflits), 5-53.

Boin A, Ekengren M and Rhinard M (2014) *Making Sense of Sense-Making: The EU's Role in Collecting, Analysing, and Disseminating Information in Times of Crisis* (Stockholm: Swedish National Defence College).

Brady H (2008) 'Europol and the European Criminal Intelligence Model: A Non-state Response to Organized Crime.' *Policing* 2 (1), 103-109.

Brand F S and Jax K (2007) 'Focusing the Meaning(s) of Resilience: Resilience as a Descriptive Concept and a Boundary Object.' *Ecology and Society* 12(1).

Brassett J, Croft S and Vaughan-Williams N (2013) 'Introduction: An Agenda for Resilience Research in Politics and International Relations.' *Politics* 33 (4), 221–228.

Brassett J and Vaughan-Williams N (2013) 'The Politics of Resilience from a Practitioner's Perspective: An Interview with Helen Braithwaite OBE'. *Politics* 33(4), 229–239.

Brown K (2014) 'Global environmental change I: A social turn for resilience?' *Progress in Human Geography* 38 (1), 107-117.

Bures O (2011) *EU counterterrorism policy: a paper tiger?* (Farnham – Burlington, VT: Ashgate).

Carrera S (2007) 'The EU Border Management Strategy. FRONTEX and the Challenges of Irregular Immigration in the Canary Islands', *CEPS Working Document*, No. 261 (Brussels: CEPS).

Comfort L K et al (2001) 'Complex Systems in Crisis: Anticipation and Resilience in Dynamic Environments.' *Journal of Contingencies and Crisis Management* 9 (3), 144–158.

Darnis J-P and Veclani A C (2011) Space and security: the use of space in the context of the CSDP (Strasbourg: European Parliament).

Davis Cross M K (2013) 'A European Transgovernmental Intelligence Network and the Role of IntCen.' *Perspectives on European Politics and Society* 14 (3), 388-402.

De Bruijne M, Boin A and van Eeten M (2010) 'Resilience: Exploring the Concept and Its Meanings.' In Comfort L K, Boin A and Demchak C C (eds) *Designing Resilience: Preparing for Extreme Events* (Pittsburgh: University of Pittsburgh Press, 2010), 13-32.

Deflem M (2006) 'Europol and the Policing of International Terrorism: Counter-Terrorism in a Global Perspective.' *Justice Quarterly* 23 (3), 336-359.

Deflem M (2010) *The policing of terrorism: organizational and global perspectives* (New York and Abingdon: Routledge).

Dunn Cavelty M, Kaufmann M, Kristensen K S (2015) Resilience and (in)security: Practices, subjects, Temporalities.' *Security Dialogue* 46 (1), 3–14.

Edwards C (2009) *Resilient Nation* (London: Demos).

Evans B and Reid J (2013) 'Dangerously exposed: The life and death of the resilient subject.' *Resilience: International Policies, Practices and Discourses* 1 (2), 83–98.

Evans B and Reid J (2014) *Resilient Life. The Art of Living Dangerously* (Cambridge and Malden, MA: Polity Press).

Fingar T (2011) *Reducing uncertainty: intelligence analysis and national security* (Stanford, CA: Stanford University Press).

Friedrichs J (2008) *Fighting Terrorism and Drugs. Europe and international police cooperation* (London and New York: Routledge).

Frontex (2013a) 'Annual Risk Analysis 2013' (Warsaw: Frontex Risk Analysis Unit)

Frontex (2013b) 'Strategic Analysis', http://frontex.europa.eu/intelligence/strategic-analysis (retrieved on 23 August 2014).

Grabo C M (2002) *Anticipating Surprise. Analysis for Strategic Warning* (Washington, DC: Joint Military Intelligence College, Center for Strategic Intelligence Research).

Grimm V and Calabrese J M (2011) 'What Is Resilience? A Short Introduction.' In Deffuant G and Gilbert N (eds) *Viability and Resilience of Complex Systems. Concepts, Methods and Case Studies from Ecology and Society* (Berlin – Heidelberg: Springer-Verlag), 3-13.

Gruszczak A (2013) 'EU Intelligence-led Policing: The Case of Counter-terrorism Cooperation.' In O'Neill M, Swinton K and Winter A (eds) *New Challenges for the EU Internal Security Strategy* (Newcastle upon Tyne: Cambridge Scholars Publishing), 16-39.

Guidetti R and Martinelli T J (2009) 'Intelligence-Led Policing - A Strategic Framework.' *The Police Chief* LXXVI (10), http://www.policechiefmagazine.org/magazine/index.cfm?fuseaction=display&article_id=1918&issue_id=102009 (retrieved on 22 March 2012).

Haag D and Anaya C B (2011) 'The first ten years of military Intelligence Support for the work of the EU.' *IMPETUS. Bulletin of the EU Military Staff* 11, 8-9.

High Representative (2011) 'High Representative Catherine Ashton visits the new EU Situation Room.' Press Release, A 286/11, Brussels, 18 July.

Holling C S (1973) 'Resilience and Stability of Ecological Systems.' *Annual Review of Ecology and Systematics* 4 (1), 1–23.

Hollnagel E (2014) 'Becoming Resilient'. In Nemeth C P and Hollnagel E (eds) *Resilience Engineering in Practice, Volume 2. Becoming Resilient* (Farnham and Burlington, VT: Ashgate), 179-192.

House of Lords (2003) EU – Effective in a Crisis?, House of Lords, Select Committee on the European Union, Session 2002-03, Seventh Report, HL Paper 53 (London: The Stationery Office).

Hukkinen J (2008) *Sustainability Networks: Cognitive Tools for Expert Collaboration in Social-Ecological Systems* (London and New York: Routledge).

Janssen M A (2007) 'Update on the Scholarly Networks on Resilience, Vulnerability, and Adaptation within the Human Dimensions of Global Environmental Change.' *Ecology and Society* 2007, 12(2), 9.

Janssen M A et al (2006) Toward a Network Perspective of the Study of Resilience in Social-Ecological Systems.' *Ecology and Society* 11 (1), 15.

Janssen M A, Schoon M L, KeW and Börner K (2006) 'Scholarly networks on resilience, vulnerability and adaptation within the human dimensions of global environmental change.' *Global Environmental Change* 16 (3), 240–252.

Johnson L K and Wirtz J J (eds) (2004) *Strategic Intelligence:Windows into a Secret World* (Los Angeles, CA: Roxbury).

Jones C. (2012) 'Secrecy reigns at the EU's Intelligence Analysis Centre.' *Statewatch* 22 (4), 1-5.

Kaplan H B (2002) 'Toward an Understanding of Resilience: A Critical Review of Definitions and Models.' In Glantz M D and Johnson J L (eds) *Resilience and Development. Positive Life Adaptations* (New York – Boston – Dordrecht – London – Moscow: Kluwer Academic Publishers), 17-83.

Kaunert C (2010) *European Internal Security - towards supranational governance in the Area of Freedom, Security and Justice?* (Manchester: Manchester University Press)**.**

Kolar K (2011) 'Resilience: Revisiting the Concept and its Utility for Social Research.' *International Journal of Mental Health Addiction* 9 (4),421–433.

Kozłowski J and Palacios-Coronel J M (2014) 'Single Intelligence Analysis Capacity (SIAC) - A Part of the EU Comprehensive Approach.' *IMPETUS. Magazine of the EU Military Staff* 17, 10-11**.**

Kølvraa C (2010) *Imagining Europe As a Global Player : The Ideological Construction of a New European Identity Within the EU* (Bruxelles: P.I.E. Peter Lang).

Lentzos F and Rose N (2009) 'Governing insecurity: Contingency planning, protection, resistance.' *Economy and Society* 38 (2), 230-54.

Manosevitz J U (2013) 'Needed: More Thinking about Conceptual Frameworks for Analysis—The Case of Influence.' *Studies in Intelligence* 57 (4), 15-22.

Miozzo A (2014) 'The practice of global crisis management.' In Pawlak P and Ricci A (eds) *Crisis rooms: towards a global network?* (Paris: EU Institute for Security Studies), 39-44.

Müller-Wille B (2008) 'The Effect of International Terrorism on EU Intelligence Co-operation.' *Journal of Common Market Studies* 46 (1), 49-73.

Neal A W (2009) 'Securitization and Risk at the EU Border: The Origins of FRONTEX.' *Journal of Common Market Studies* 47 (2), s. 333-356.

Neocleous M (2012) '"Don't be Scared, Be Prepared": Trauma, Anxiety, Resilience.' *Alternatives* 37 (3), 188–198.

Nimark A and Pawlak P (2014) 'Upgrading the Union's response to crises.' In Pawlak P and Ricci A (eds) *Crisis rooms: towards a global network?* (Paris: EU Institute for Security Studies), 107-115.

Norheim-Martinsen P M (2013) *The European Union and Military Force. Governance and Strategy* (Cambridge: Cambridge University Press).

Peterson M (2005) *Intelligence-Led Policing: The New Intelligence Architecture* (Washington, DC: Bureau of Justice Assistance, U.S. Department of Justice), https://www.ncjrs.gov/pdffiles1/bja/210681.pdf (retrieved on 22 March 2012).

Ratcliffe J (2008) *Intelligence-Led Policing* (Cullompton and Portland, OR: Willan Publishing).

Richards J (2010) *The Art and Science of Intelligence Analysis* (Oxford – New York: Oxford University Press).

Rogers P (2015) 'Researching resilience: An agenda for change.' *Resilience: International Policies, Practices and Discourses* 3 (1), 55-71.

Rumsfeld D (2011) *Known and Unknown. A Memoir* (New York: Sentinel).

Rumsfeld D (2013) *Rumsfeld's Rules. Leadership Lessons in Business, Politics, War, and Life* (New York: HarperCollins Publishers).

Schmidt J (2015) 'Intuitively neoliberal? Towards a critical understanding of resilience governance.' *European Journal of International Relations* 21 (2), 402–426.

Seiffarth O (2011) 'The Development of the European Border Surveillance System (EUROSUR).' In Burgess J P and Gutwirth S (eds) *A Threat Against Europe? Security, Migration and Integration* (Brussels: VUBPRESS), 133-151.

Sullivan J P (2007) 'The New Great Game: Military, Police and Strategic Intelligence for Global Security.' *Journal of Policing, Intelligence and Counter Terrorism* 2 (2), 15-29.

Van Breda A DP (2001) *Resilience Theory: A Literature Review* (Pretoria: South African Military Health Service), http://www.vanbreda.org/adrian/resilience/resilience_theory_review.pdf (retrieved on 12 August 2015)

Van Buuren J (2009) *Secret Truth. The EU Joint Situation Centre* (Amsterdam: Eurowatch).

Van Duyne P C (2007) 'OCTA 2006: the unfulfilled promise.' *Trends in Organised Crime* 10 (2), 120-128.

Villadsen O R (2000) 'Prospects for a European Common Intelligence Policy.' *Studies in Intelligence* 44 (9), 81-94.

Walsh B (2013) 'Adapt or Die: Why the Environmental Buzzword of 2013 Will Be *Resilience'. Time Magazine Online*, 8 January, http://science.time.com/2013/01/08/adapt-or-die-why-the-environmental-buzzword-of-2013-will-be-resilience/ (retrieved on 14 August 2015).

Walker J and Cooper M (2011) 'Genealogies of Resilience: From systems ecology to the political economy of crisis adaptation.' *Security Dialogue* 42 (2), 143–160.

Walker B, Holling C S, Carpenter S R and Kinzig A (2004) 'Resilience, Adaptability and Transformability in Social–ecological Systems.' *Ecology and Society* 9 (2).

Waltz E (2003) *Knowledge Management in the Intelligence Enterprise* (Boston-London: Artech House).

Wears R L and Webb L K (2014) 'Fundamental on Situational Surprise: a Case Study with Implications for Resilience.' In Nemeth C P and Hollnagel E (eds) *Resilience Engineering in Practice, Volume 2. Becoming Resilient* (Farnham and Burlington, VT: Ashgate), 33-46.

Webster's (1986) *Webster's New World Dictionary of the American Language*, 2nd College edition (New York: Prentice Hall).

Weick K E, Sutcliffe K and Obstfeld D (2002) 'High reliability: The power of mindfulness.' In Hesselbein F and Johnston R (eds) *On high performance organizations* (San Francisco: Jossey-Bass), 7–18.

Wheaton K J and Beerbower M T (2006) 'Towards a New Definition of Intelligence.' *Stanford Law & Policy Review* 17 (2), 319-331.

White J R (2009) *Terrorism and Homeland Security* 6th ed (Belmont, CA: Wadsworth Cengage Learning).

Wildavsky, A (1988) *Searching for Safety* (New Brunswick, NJ: Transaction Publishers).

Xu L and Marinova D (2013) 'Resilience thinking: a bibliometric analysis of socio-ecological research.' *Scientometrics* 96(3), 911–927.

Zoutendijk A J (2010) 'Organised crime threat assessments: a critical review.' *Crime, Law and Social Change* 54 (1), 63-86.