Clingendael

Netherlands Institute of International Relations

Clingendael Report

Civil-Military Capacities for European Security

Margriet Drent
Kees Homan
Dick Zandee

Civil-Military Capacities for European Security

Clingendael

Netherlands Institute of International Relations

Civil-Military Capacities for European Security

Margriet Drent
Kees Homan
Dick Zandee

Design: Textcetera, The Hague
Print: Gildeprint, Enschede

Clingendael Institute
P.O. Box 93080
2509 AB The Hague
The Netherlands

Email: info@clingendael.nl
Website: http://www.clingendael.nl/

Content

Executive summary

In the last two decades the European Union has created separated policies, institutions and capacities for external and internal security. In the meantime the world's security environment has changed fundamentally. Today, it is no longer possible to make a clear distinction between security outside and within Europe. Conflicts elsewhere in the world often have direct spill-over effects, not primarily in terms of military threats but by challenges posed by illegal immigration, terrorism, international crime and illegal trade. Lampedusa has become a synonym for tragedy. Crises and instability in Africa, the Middle East and elsewhere in the world provide breeding grounds for extremism, weapons smuggling, drugs trafficking or kidnapping. Libya has been liberated from dictatorship but the country is still in chaos. Mali was about to become another Afghanistan. Piracy is interrupting the freedom of the seas on which European trade is so dependent. Maritime security, border security and cyber security cannot be categorised as either external or internal security issues – they belong to both.

In practice, however, internal and external security actors still live in separated worlds. At the Union level the institutional divide between intergovernmental and supranational responsibilities is an important factor. Foreign policy and defence remain firmly in the hands of national governments, while for all other sectors of government sovereignty is at least partly given to the Union level. Therefore, the European Council should define objectives and issue guidance for *slashing legal* barriers which block *structural coordination between internal and external security actors.* Equally important are the stove-piped bureaucratic structures in member state capitals, dealing with external and internal security. A fear of opening up one's own area of responsibility and competence to another ministry – in particular to the military – plays a significant role. Even member states with a whole-of-government approach to their national security have not been able to implement the concept properly. Other member states even lack such an approach today. The *EU needs an integrated security approach* but the *same has to happen at the national level.*

In her report in preparation for the December 2013 European Council on Security and Defence the High Representative Catherine Ashton has clearly concluded that the distinction between external and internal security is breaking down. She is looking for civil-military synergies and has made a plea to extend the comprehensive approach to capabilities. The European Commission

has made practical proposals, for example to co-fund defence research projects in dual-use technologies. The European Council should support these proposals and task the Brussels actors to implement them by defining concrete objectives and milestones. In particular the scope for *EU-owned dual-use remotely piloted aircraft systems (unmanned drones)* should be explored. They can fly to monitor Europe's long land borders and check the sea areas, but the same assets can be deployed by the military for operations in Africa or elsewhere.

Three areas stand out to realise civil-military synergies in capabilities. The first area is maritime security, which involves national and international, civil and military players who so far are not working together in a structural manner. The EU maritime security strategy, delayed for years due to turf battles between the various actors, should be completed quickly. The strategy has to be *global, civil-military and comprehensive*. Its governance has to be based on the *legal responsibilities* of the actors involved and its *structure* should be *integrated* to the extent possible in terms of operational tools, civil and military.
Maritime surveillance stands out as the capacity which seems to have advanced furthest in the direction of a civil-military integrated approach. Regional civil-military networks have already been developed and many pilot projects have taken place. What is now needed is a European-wide network, connecting existing networks in order to share all available data from national and international sources, both military and civil. The *European Commission's Common Information Sharing Environment (CISE)* should provide the *umbrella network* with the *European Maritime Safety Agency (EMSA)* as the logical agency *to provide the operational leg*. The European Council should give the necessary guidance, including to change the legal provisions which now separate the military and civilian actors. Member states should extend their *pooling and sharing* activities to *civil-military capacities and assets like maritime patrol aircraft*, to start with in regional clusters for the Baltic Sea, the North Sea, the Atlantic approaches and the Mediterranean.

The second area is border security. As modern border management involves technology and equipment that shows to a large extent an overlap with the needs of modern armed forces, there is clear potential for synergies. Member states are already supporting the EU's border control agency Frontex with military assets, in particular in the Mediterranean. Instead of ad hoc solutions more structural cooperation should be realised. This requires both sides to act. Defence ministries should incorporate the *availability of naval and other assets* for Frontex in their *planning*. For the acquisition of its own assets Frontex should take into account *standardisation and interoperability* with the military and civilian capacities of member states. Frontex arrangements on the *co-ownership of*

equipment with member states could be applied to other dual-use assets which the Commission might acquire, such as *unmanned drones*.
The new European border surveillance system (Eurosur) will start its operational phase in December 2013. Its data exchange network is a major step forward in support of border security in the EU. Other actors, including the *member states' armed forces*, should be *connected to Eurosur* for a two-way street exchange of information.
The border management area is developing at a fast pace. Although complications regarding legal frameworks, stove-pipe policies, differing competences, modus operandi, sovereignty issues, ethical objections and political priorities make it difficult for the defence sector to hop onto this speeding train, the potential is clear. The two worlds are mutually reinforcing, but one of the first problems to overcome seems to be that they are still relative strangers.

Cyber security is the third area for civil-military integration. The benefits of coordination and cooperation across the EU on cyber security, including between civilian and military actors, is clear. However, an awareness of the threats, technological competences to deal with them as well as internal structures show a wide variety among member states. The European Union should play an important role in *setting and discussing norms* and debating *resilience measures* to support *civil and military authorities in member states*. The EU Cyber Security Strategy will only succeed if *turf battles* between the various actors come to an end and the envisaged *action plan* and the *Directive* of the Commission are agreed upon and implemented.
National cyber security strategies should allow for *linking* national assets and mechanisms *to EU-level cyber arrangements*. European military and civil cyber security stakeholders should work *much closer* together to boost Europe's network and information security (ENIS). As military cyber security measures show a mixed and generally immature picture, the recommendations of a European Defence Agency study should be implemented, in particular with regard to doctrine, training and interoperability.

Introduction

The European Union deploys military forces and civilian experts to prevent or end conflicts and to create conditions for restoring peace and stability. These capabilities, made available by the member states, are increasingly being deployed together with the European Union's communitarian assets such as humanitarian assistance, development aid, reconstruction and rehabilitation tools. Deploying all these instruments together in the comprehensive approach to crisis management is the EU's hallmark and it starts to produce positive results in areas like the Horn of Africa.

Yet, when it comes to security within the EU, civilian and military capacities remain strictly separated. Perhaps this made sense in 2000 when defence was introduced in the EU. The military protection of Europe was a NATO responsibility. Thus, the EU would focus solely on crisis management outside the Union's borders. Nearly fifteen years later this limitation of European defence to external action seems to be outdated. Increasingly, Europe's security is affected by spill-over effects of crises in its immediate neighbourhood or even further away. Terrorism, illegal immigration, international crime and drugs trafficking have impacted security in European countries, from Lampedusa to London and from the Aegean to Madrid. Such threats and challenges to the EU's internal security are likely to increase in a future world characterised by tensions and potential conflict, in particular in the arc of instability reaching from the Caribbean through northern Africa to the Middle and Near East. Climate change and disasters, man-made or natural, also affect the security of the EU and its citizens.

Internal security is primarily the responsibility of Justice and Home Affairs. Other departments such as Transport will be involved when it comes to maritime security. Defence and the armed forces mainly have supportive roles. EU member states have their own arrangements for military support to civilian authorities responsible for internal security – state prosecutors, the police, border control organisations – or for the safety of adjacent sea areas (the coast guard). But at the European level such arrangements are lacking while, at the same time, internal and other security responsibilities are being transferred to the EU on a step-by-step basis. The capacities needed to deal with external and internal security threats and challenges are developed, deployed and directed through separate channels. For example, EU information exchange networks for maritime security or for border control are separated from military networks. EU agencies

such as Frontex have called on member states to support their operations with military means, but only on an ad hoc basis.

A lack of structural coordination between internal and external security actors in the EU entails risks. Military assets may not be available when needed because they are deployed elsewhere or engaged in training and exercises. This will have an effect on response time – of particular importance when dealing with disasters which always occur suddenly and unexpectedly. Available military assets might not be the most suitable for security tasks under civilian control. This could be prevented if specific requirements for carrying out these tasks would have been taken on board when developing these capacities. A lack of civil-military standardisation in areas like communications, observation, transport and medical support can have dramatic consequences, in the worst case even leading to a loss of life.

European security in the wider sense would profit from a more coordinated and integrated way of developing and using civil-military capacities. The question is how this goal can be reached. This study will focus on the development and use of civilian and military capabilities for European security in a more coherent and structured way. Chapter 1 will focus on the external-internal security gap. Why does it exist? What has been undertaken so far to close the gap, by nations as well as at the European level? What difficulties have been encountered in this process? In the following chapters the focus is on three case studies. Chapter 2 looks at maritime security, in particular how civilian assets and navies could be linked more systematically at EU level. Chapter 3 addresses the issue of border security. Military assets of several member states have already been deployed in support of EU border control activities. This experience can be used when defining more permanent civil-military arrangements. Capability development is equally important as some of the required high technology assets – such as unmanned aircraft – are dual-use systems. In chapter 4 the case study is cyber security, which in recent years has become a major security concern to national, international, civilian and military authorities alike. Chapter 5 lists the conclusions and provides a set of recommendations.

1 The external-internal security gap

During the Cold War the security of the West was based on the transatlantic Alliance. Security was primarily defined as defence against an outside threat of massive armed forces. NATO was the guardian of collective defence at the Iron Curtain. After the fall of the Berlin Wall the Alliance engaged in crisis management operations outside its Treaty area. In 2000 the European Security and Defence Policy (ESDP) – since the Lisbon Treaty entered into force renamed as the Common Security and Defence Policy (CSDP) – was launched in the European Union. It would be limited to crisis management in areas external to the EU. The territorial defence of Europe continued to be NATO's responsibility.

A gap created

ESDP had no relationship with the internal security of the European Union, which was primarily seen as 'a matter of the interior', meaning the Justice and Home Affairs (JHA) sectors.[1] It reflected the traditional division of responsibilities of the departments most involved: on the one hand, Foreign Affairs and Defence, responsible for 'abroad' and 'military operations', and, on the other, Justice and Home Affairs bearing responsibility for law and order within national territory. In the EU the external-internal separation also had institutional aspects. ESDP was intergovernmental, based on decision–making by unanimity in the Council. Member states delivered the assets – military forces and civilian capabilities such as police officers – for ESDP operations. The EU's internal security cooperation in the JHA areas moved from a mixture of intergovernmental and communitarian responsibilities in the nineties to a predominantly Community (Union) matter under the Lisbon Treaty. Other sectors of cooperation with security aspects – space, maritime safety, infrastructure protection and many others – also belong to the communitarian agenda, financed by the Community budget and controlled by the European Parliament.

A gap had been created by separating the EU's external and internal security policies and structures. More importantly, the planning of the capabilities

1 Since the Amsterdam Treaty known as the 'Area of Freedom, Security and Justice' (AFSJ). See chapter 3 for details. In this chapter the better-known acronym JHA will be used.

needed for external and internal security tasks was organised through separate channels. EU defence cooperation was set up in isolation from Europe's internal security while the dividing line between external and internal security would only become weaker.

Impact of terrorism

The terrorist attack on the twin towers in New York (2001), the train bombings in Madrid (2004) and the underground explosions in London (2005) were major shocks that brought a new sense of insecurity into the interior of the Western countries. Suddenly, it became clear that a lack of security elsewhere in the world could result in importing its effects to the streets of American and European cities. 'Terrorism doesn't recognise borders' became a popular expression. In the EU, counter-terrorism was developed as an important area of cooperation in JHA competence. Although the external aspect could not be denied – the roots of terrorism were situated outside the EU – the involvement of ESDP in the fight against terrorism remained limited. The first EU Counter-Terrorism Coordinator concluded in 2008 that "Counter-terrorism has not been mainstreamed into the civilian and military crisis management missions of the Union" and that "Presidency efforts to promote cross-Pillar synergies in the Council, notably between Justice and Home Affairs Ministers and Ministers of Foreign Affairs and Defence, have been less than consistent."[2]

Wider security

The European Security Strategy (ESS) of 2003 recognised that security could no longer be perceived in the narrower and traditional sense: "The post Cold War environment is one of increasingly open borders in which the internal and external aspects of security are indissolubly linked." The list of key threats was not limited to conflicts and state failure – the focus of ESDP – but incorporated, for example, terrorism and organised crime. Concerning the latter the ESS stated: "This internal threat to our security has an important external dimension: cross-border trafficking in drugs, women, illegal immigrants and weapons form a large part of the activities of criminal gangs." The Union had to respond with a mixture of instruments, deploying them in a more coherent manner.[3] But as far as the external-internal connection was concerned practice did not follow theory. The 2008 ESS update drew the sober conclusion that "We need to improve the way in which we bring together internal and external dimensions.

2 Gijs de Vries, 'The nexus between EU crisis management and counter-terrorism', in S. Blockmans, ed., *The European Union and Crisis Management*, The Hague, 2008, p. 356.

3 *A Secure Europe in a Better World – European Security Strategy*, Brussels, 12 December 2003.

Better co-ordination, transparency and flexibility are needed across different agencies, at national and European level. (…) Progress has been slow and incomplete." In the same document cyber security, energy security and climate change were added to the list of threats and challenges to European security interests.[4]

Early practical steps

In the civil protection area the first step was taken for arrangements with regard to military support. However, the result – a database of available military assets and capabilities of the member states collected by the EU Military Staff (EUMS) – remains limited until today. Not all EU member states answered the call by the EUMS and the database is based exclusively on voluntary contributions.

Other practical steps forward to connect the needs of military and civilian users were made in capability development projects of the European Defence Agency (EDA). Soon after its operational start in early 2005 the Agency launched several projects for which dual-use requirements were taken into account, such as for Software Defined Radio. In subsequent years the EDA would expand this area of work into connecting civil and military needs and activities in areas like satellite communications and observation, intelligence, medical support, unmanned aircraft systems, transport and many others. Close links with the European Commission but also with many EU agencies and with the European Space Agency were set up long before the Lisbon Treaty entered into force. With its practical way of working – keeping some distance from the political-diplomatic circles of the Council Lipsius Building – the EDA was able to run ahead in closing the EU's external-internal security capabilities gap.

National responses

The changing security environment resulted in the review of national strategies or policies. European capitals started to recognise that external and internal security were closely interlinked. Nations had to face threats and challenges from outside and inside, generated by states and by non-state actors, targeted at military and civilians alike and thus requiring government-wide responses.

A review of member states' responses delivers a scattered landscape. There are different concepts and orientations of national security strategies across

4 *Report on the Implementation of the European Security Strategy – Providing Security in a Changing World*, Brussels, 11 December 2008.

Europe. The British National Security Strategy (NSS, 2010) and the Spanish Security Strategy (2011) come closest to an integrated or comprehensive whole-of-government approach to deal with the melting of external and internal security risks and challenges.[5] Implementation is another matter. In the British case the Joint Committee of the House of Lords and the House of Commons plays an important role in assessing progress and making recommendations for improvement. It has been critical regarding progress with the whole-of-government approach in practice. The committee's primary concern is the mismatch between Britain's National Security Strategy and the decisions taken to restructure the British Armed Forces.[6] Two years later, the Joint Committee was more positive but it nevertheless concluded: "(..) we are not yet convinced that the existence of the NSS is making the contribution that it should: enabling Government to work as a co-ordinated whole."[7]

France has a whole-of-government type of national security strategy, but it is embedded in the White Books on Defence and Security which underlines the dominating military thinking in Paris when addressing security. The 2013 *Livre Blanc* of President François Hollande makes a plea for "the European dimension of national security" and launches practical proposals, e.g. for the creation of an EU-integrated maritime surveillance system or for pooling assets made available by member states for the border control activities of Frontex.[8] This is a clear call for European defence cooperation in support of EU internal security.

Germany has no national security strategy but claims to have a whole-of-government approach, including the supporting role of the armed forces in internal security tasks. The Defence Policy Guidelines (2010) underscore the need for "a national, comprehensive and coordinated security policy that includes political and diplomatic initiatives as well as economic, development policy, police, humanitarian, social and military measures."[9] The Bundeswehr can support – and in fact has done so on many occasions – the Ministry of Interior and other ministries in case of internal security threats or disasters such as flooding. Without a national security strategy Berlin has made the necessary

5 *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, Presented to Parliament by the Prime Minister by Command of Her Majesty, October 2010. *Spanish Security Strategy – Everyone's responsibility*, Gobierno de España, Madrid 2011.

6 Joint Committee on the National Security Strategy, *First review of the National Security Strategy 2010*, First Report of Session 2010-12, HL Paper 265 HC 1384.

7 *The Work of the Joint Committee on the National Security Strategy in 2012*, Second Report of Session 2012-13, HL Paper 115 HC 984.

8 *Livre Blanc Défense et Sécurité Nationale 2013*, Paris 2013.

9 *Defence Policy Guidelines: Safeguarding National Interests Assuming International Responsibility – Shaping Security Together*. German Ministry of Defence, Berlin, 27 May 2011.

arrangements for the supporting role of the armed forces in internal security tasks. However, for maritime security the case is less clear (see chapter 2).

The National Security Strategy of the Netherlands (2007) recognises the connection between external and internal security and the need for cooperation between all government departments in an integrated approach.[10] However, in practical terms tools and measures are mainly developed by the traditional internal security departments. The continuation of separated worlds in The Hague has been reinforced by the new International Security Strategy of 2013, developed by the Foreign Ministry.[11] It also points to the linkage between external and internal security, but in terms of policy and measures it is focused on foreign policy and defence only. There is no doubt that the stove-piped government structure of the Netherlands with a relatively weak Prime Minister's office and strong sector departments plays an important role in the difficulty of bringing about a whole-of-government approach. On the other hand, the Dutch are champions in practical solutions. Under the programme 'Intensifying Civil-Military Cooperation' (ICMS)[12] a package of minimum military capacities is being made available to the Ministry of the Interior and the Ministry of Security and Justice.[13] There are positive examples of civil-military cooperation in areas like maritime security, disaster management, countering terrorism and cyber security – some of which will be mentioned in the case studies of this publication.

In other European countries the situation is equally challenging, as national security strategies are outdated or absent. The resulting picture is a wide variety of responses in a landscape of growing interconnection between external and internal security. Logically, this also leads to different national arrangements for bridging the gap between civil and military means to deal with the new security environment – as the case studies in chapter 2-4 will show.

EU responses

Lisbon Treaty

On 1 December 2009 the Lisbon Treaty entered into force. It brought major institutional changes, such as ending the old pillar structure and introducing a double-hatted High Representative and Vice-Presidency of the European

10 *Strategie Nationale Veiligheid*, 2007. The Strategy is regularly assessed and updated. Translation into English by the authors.
11 *Veilige Wereld, Veilig Nederland. Internationale Veiligheidsstrategie*, 21 juni 2013.
12 In Dutch: Intensivering Civiel Militaire Samenwerking (ICMS).
13 In 2010 the Rutte-1 Government renamed the Ministry of Justice as the Ministry of Security and Justice.

Commission. The Common Security and Defence Policy's focus remained the same, but the Treaty opened the box for deploying armed forces within the EU. The Solidarity Clause created the possibility of making military resources available to assist a member state under terrorist attack or hit by a disaster. The Mutual Defence Clause even obliges member states to provide aid and assistance to a member state which is the victim of major aggression. In the area of funding – such as for research and development – the Lisbon Treaty is offering scope for joint funding by member states and the Commission of technology projects for dual-use application.

It took several years before the scope of the Lisbon Treaty would be explored. The EDA's campaign of 2010 to activate article 185 failed. Traditional forces inside the European Commission, in particular those driven by legal principles, wanted to stick to the strict separation of military and civilian-driven research. They were successful. A solution was found in the European Framework Cooperation (EFC) for research and technology, also prepared by the European Defence Agency. The EFC allowed for the coordination of EDA programmes with security research financed by the Union – under the 7th Framework Programme – and with the European Space Agency as the third EFC partner. In a sense the EFC established a 'back-to-back mode' for the coordination of dual-use technology investment in order to prevent duplication. Defence ministers tasked EDA to develop EFC programmes in the areas of CBRN (Chemical, Biological, Radiological, Nuclear) protection, unmanned aircraft systems and situational awareness. Currently, only in the CBRN area is an EFC programme up and running.[14]

Internal Security Strategy

In February 2010 the Council adopted an Internal Security Strategy, setting out the challenges, principles and guidelines for how to deal with these issues in the EU.[15] Its focus is on the better coordination of activities in the JHA area. The Strategy also addresses the linkage with external security and was supplemented by an action plan by the end of 2010.[16] Five priority areas were identified: international criminal networks, terrorism, cyber security, border security and disasters. The potential use of the military assets of the member states for internal security tasks is not mentioned. The implementation of the

14 *Joint Investment Programme CBRN*. See: www.eda.europa.eu.

15 *Internal Security Strategy for the European Union: Towards a European Security Model*, Council Document 5842/2/2010.

16 *Communication from the Commission to the European Parliament and the Council. The EU Internal Security Strategy in Action: Five Steps towards a more secure Europe*, COM(2010)673 final, Brussels, 22.11.2010.

Action Plan is assessed annually by the Commission. It is striking that even the deployment of military assets, such as for the EU's border control activities in the Mediterranean, have not been mentioned in the assessment reports.[17] It proved that the use of military capacities for communitarian tasks was still considered as a sensitive matter by the JHA actors.

Oversight of the Internal Security Strategy's implementation is provided by the Standing Committee on Operational Cooperation on Internal Security (COSI), created by the Lisbon Treaty. It consists of high-level officials from EU States' Ministries of Home Affairs and of Commission representatives. Cooperation with bodies responsible for EU external security is not mentioned. The European Commission's Action Plan referred to internal coordination with the European External Action Service and also to regular meetings of COSI and the Political and Security Committee (PSC, the EU's committee for Common Foreign and Security Policy, including CSDP). The two committees have developed a road-map for strengthening ties between the CSDP and actors dealing with Freedom, Security and Justice "and to further develop synergies in other areas such as cyber security, critical infrastructure protection and counter-terrorism." Two COSI-PSC meetings took place in 2012 (focused on the Western Balkans, Sahel and Libya) and one in February 2013 (on Mali).[18]

Solidarity Clause

At the end of 2012 the High Representative and the European Commission forwarded a joint proposal on the arrangements for the implementation of the Solidarity Clause, as asked for in art. 222 of the Treaty on the Functioning of the European Union (TFEU).[19] The proposal defines the geographic scope, the activation mechanism and the response arrangements for cases of disasters and terrorist attacks within EU territory, whether on land, sea or in the air. The Clause applies irrespective of whether the crisis originates within or outside the EU. The initiative to activate the Clause lies with member states. The Clause is supposed to be activated only in exceptional circumstances and when a member state sees its own capacities overwhelmed. In such a case the High Representative and the Commission will propose the response package, which can consist of Union crisis response instruments and, if needed, additional measures by member states. In the latter case the Council will have to take

17 See for example: *Communication from the Commission to the European Parliament and the Council. Second Report on the implementation of the EU Internal Security Strategy*, COM(2013)179 final, Brussels, 10.4.2013.

18 *Communication from the Commission* (see footnote 17), p. 17.

19 *Joint proposal from the European Commission and the High Representative of the Union for Foreign Affairs and Security Policy on the arrangements for the implementation by the Union of the Solidarity Clause*, 18124-12 JOIN(12)39, 21 December 2012.

a decision. If military support is needed a separate proposal will be forwarded to the Council, based on the relevant Treaty provisions.

The joint proposal makes clear that the Solidarity Clause is an option of last resort for a member state drawing the conclusion that its own means are not sufficient to deal with the consequences of a terrorist attack or a disaster. As such the text – still under consideration in the Council bodies to prepare a Council decision – seems to reflect a rather restricted interpretation of the Treaty's article 222. Furthermore, details are lacking about the potential scope and scale of member states' contributions. The article 222 language to 'act jointly' and to 'assist' one another even seems to be the last phase of a last resort measure. The same restrictive interpretation applies to military support. The Treaty text offers wider scope for making available military resources by member states which almost seems to have been neglected in this provision.[20] Complicated and time-consuming decision-making through a Council decision is contradictory to the emergency nature of delivering support. The important contribution of specialised military capacities, for example in the case when CBRN explosives are involved in an accident or a terrorist attack – is apparently neglected. The same might apply to the destruction of critical infrastructure – calling in engineering capacities of the military. Military transport helicopters might become a critical asset in cases of large areas being flooded or when earthquakes occur.

The most likely kinds of risks to European security are those covered by the Solidarity Clause, yet the member states seem reluctant to embrace the full potential of Treaty article 222. When the founding fathers of the Treaty's text will see the Council decision – assuming its final version will not deviate too much from the proposed text – they might be disappointed. An opportunity may be missed to create new international security arrangements which are absent at the moment.

December 2013 European Council

In October 2013 the EU High Representative Catherine Ashton delivered her final report preparing for the European Council on security and defence in December of the same year.[21] The first part of the report contains a description of the strategic context, which in a nutshell updates the European

20 'Whereas' (15) of the draft Solidarity Clause Council decision even states bluntly: "This decision has no defence implications".

21 *Preparing the December 2013 European Council on Security and Defence – Final Report by the High Representative/Head of the EDA on the Common Security and Defence Policy*, Brussels, 15 October 2013. See: www.eeas.europa.eu.

Security Strategy and its 2008 update. It depicts a world which "as a whole faces increased volatility, complexity and uncertainty". The report refers to "a multipolar and interconnected international system (which) is changing the nature of power. The distinction between internal and external security is breaking down." The report lists various proposals and actions to strengthen CSDP. Cyber, space and energy are specifically mentioned. Maritime security and border security are also listed under the heading CSDP as integral parts of the EU's security. Concerning capabilities the High Representative states that "Pioneer projects have been promoted to develop capabilities that have both military and civil applications. They are designed to harness synergies in the military and civil domains; maximise dual-use technologies; generate economies of scale; and extend the comprehensive approach into the area of capabilities development." Remotely piloted aircraft systems (RPAS)[22] receive particular attention as they offer a broad spectrum of military and civilian application. Other dual-use capacities to which member states should commit are satellite communications, cyber defence and satellite imagery. Furthermore, Ashton has announced to "continue to strengthen ties between CSDP and Freedom/Security/Justice actors", for example by the greater involvement of EU agencies (such as Frontex) in CSDP missions. The High Representative's report is not only the latest but also the most comprehensive effort to bring external (CSDP) and internal security together, including in terms of civil-military capacities for European security.

The European Commission has also launched a series of proposals for reforming the defence and security sector in preparation for the same December 2013 European Council meeting. The Communication points to the growing involvement of the Commission in defence matters beyond the traditional sectors of the open market and industry. Naturally, there is a strong focus on strengthening dual-use capabilities by promoting civil-military standards, by exploring synergies for dual-use research and technology, by opening up the possibility to finance defence-related research outside the scope of Horizon 2020[23], by stepping up the development of capabilities in civil-military overlapping areas like information sharing for maritime surveillance and space-related capacities, and

22 Remotely piloted aircraft systems (RPAS) is another term for unmanned aerial vehicles (UAV) or unmanned aircraft systems (UAS).

23 The Horizon 2020 research programme – for the years 2014-2020 – is the successor of the 7th Framework Programme (FP7). Horizon 2020 has a financial envelope of just over € 80 billion while €50.5 billion has been spent under FP7 in the timeframe 2008-2013.

by forwarding a proposal "for which capability needs, if any, could best be fulfilled by assets directly purchased, owned and operated by the Union". [24]

All these proposed actions are relevant to increase civil-military capability cooperation, but two of them draw particular attention. Firstly, the possibility of Union financing for defence-related research, possible under art. 185 TFEU. With the Communication the European Commission has changed its position. It now accepts that defence research can be financed by the Union budget through joint research funding with the member states' defence ministries. This is an important breakthrough which should allow for even more streamlined European dual-use technology investment. The second important element is the future acquisition, ownership and operational deployment of dual-use capabilities by the Union – read: by EU agencies like Frontex. There is a whole range of such capabilities, from space assets to drones, helicopters, medical support, information and communications. Commissioner Michel Barnier has mentioned the possibility of a European drones fleet to reinforce European defence capabilities and to decrease dependency on the two countries currently dominating the market (Israel and the United States). The Commission could support such a European drone programme by promoting research and harmonising legislation on airspace, which is different in every member state. Furthermore, Barnier mentioned hospital ships, aircraft carriers, maritime surveillance drones, cyber security facilities and laboratories related to CBRN as equipment "that could be jointly acquired and used if necessary."[25]

The gap: smaller but not closed

The external-internal security gap, created around 2000, has been narrowed under the influence of the changing security environment. However, the full potential offered by the Lisbon Treaty still has to be completely used. Policies and practical measures and arrangements still reflect predominantly separated worlds. This is particularly the case for operational cooperation, where coordination, comprehensiveness and coherence have been improved, but mainly within the internal security and external relations fields and not so much between them. With regard to capability development the situation looks better. From the start EDA pursued a policy of bringing military and civilian needs and requirements together. It happened without much political debate as it seemed the logical way forward to develop dual-use capabilities. Increasingly,

24 *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – Towards a more competitive and efficient defence and security sector*, COM/2013/0542 final, 24 July 2013.

25 *Barnier urges Europeans to build their own drones*, EurActiv.com, 24 July 2013.

the European Commission also became a promoter of connecting civilian user needs to those of the military, be it with great care being taken not to cross legal red lines. The most recent proposals by the Commission for the December 2013 European Council point to pushing the red line somewhat further away, in particular in the area of combining Union and member states' defence research in dual-use technologies.

A major factor blocking fusion of external and internal security policies and instruments in the EU is the institutional divide between intergovernmental and supranational responsibilities. But equally important driving forces are the separated stove-pipes in capitals, dealing with external and internal security. The fear of opening up one's own area of responsibility and competence to another ministry – in particular to the military – plays an important role. The traditional 'secrecy' culture of the ministries of defence does not help to raise understanding among other ministries either. Even member states which have launched several years ago a whole-of-government approach for their national security have not been able to implement the concept properly. Other member states even lack such an approach. Thus, there is a great need – not only at the national level but also Europe-wide – to realise a more coherent, systematic and truly coordinated approach to developing civil-military capabilities for an integrated European security.


RAF
RESCUE
Lifeboats

2 Case study maritime security

The importance of the seas for Europe

Europe's security is highly dependent on the seas. The EU has a coastline of over 90,000 kilometers. The continent is surrounded by five regional sea basins (Baltic, North, Atlantic, Mediterranean and Black Seas). Overseas territories are located as far as in the Pacific Ocean. Approximately 90% of the EU's external trade and over 40% of its internal trade is transported by sea. Maritime transport is the lifeblood of Europe's welfare. Energy production and transport, fisheries, the environment and climate change: they are all related to maritime security in one way or another.

The seas also play a crucial role in bringing security threats and challenges to Europe. Illegal immigration across the Mediterranean has grown as the Arab Spring unfolded. Sea transport plays a major role in drugs trafficking and illegal trade, including in arms and munitions. Many of the ships used for smuggling have also been involved in collisions, pollution or other incidents. Further away piracy has generated naval interventions. With EU anti-piracy Operation Atalanta off the Somalia coast, ongoing since 2008, European defence also includes a maritime dimension. More recently piracy has also emerged in other areas such as in waters adjacent to West Africa. But it is not the only threat to the freedom of the seas. A detailed study conducted for the European Parliament's Sub-Committee on Security and Defence concludes that the global maritime system is becoming more vulnerable and less resilient. The study lists six emerging challenges: failed and collapsing states in the EU's neighbourhood, in particular in the Middle East; international terrorism, including hijacking and direct attacks; piracy; illegal immigration, in particular along Mediterranean, West African and Black Sea routes; transnational crime, such as drugs and arms trafficking; and environmental security risks. Based on these various maritime threats the study draws the conclusion that "the EU therefore needs a comprehensive strategy that acknowledges the interconnectedness of different threat factors."[26]

26 *The Maritime Dimension of CSDP: Geostrategic Maritime Challenges and Their Implications for the European Union*, Directorate-General for External Policies, Policy Department, January 2013, p. 21.

The information sharing gap

Maritime security is highly dependent on maritime surveillance data exchange. The problem is that at national and EU levels responsible authorities of the different sectors all assemble information for their own purposes. Different legal frameworks and provisions hamper the exchange of information.
After several years of research the Commission concluded that maritime surveillance is the responsibility of about 400 public authorities at the national and EU level. They carry out seven maritime surveillance functions: border control, customs, defence, fisheries control, general law enforcement, maritime environment, and maritime safety and security. Information is being handled in about 20 different systems. They all collect information to build up their own sector awareness picture, but information sharing between them is weak as "of the total information required on a regular or sporadic basis by all seven user communities, 40% to 90% is not yet made systematically available."[27]
The consequences are easy to define: the maritime situational awareness of all seven sectors is incomplete, actions by their authorities remain uncoordinated and taxpayer's money is being wasted by expensive overlapping investments in assets like radars, ships or surveillance aircraft.

While the Commission was conducting its research in the context of the Integrated Maritime Policy (IMP) the European Defence Agency had mandated an external team to provide a study on maritime surveillance. Five 'Wise Pens' – retired Vice-Admirals from France, Italy, Germany, Spain and the United Kingdom – delivered their report in the spring of 2010.[28] They concluded that gradual improvements in co-ordination and integration are affordable and technologically not difficult. The obstacles to better information sharing "are essentially cultural and organisational." The Team strongly argued for replacing the principle of "the need to know" by "the need to share" and "a responsibility to provide obligation". In the autumn of 2010 the Wise Pen Team delivered a progress report[29] in which they repeated many of the earlier conclusions and added ideas and proposals for an overarching European Maritime Security Strategy. The Vice-Admirals' call came after the Foreign Affairs Council of April 2010 had invited "the High Representative, together with the Commission and the Member States, to undertake work with a view to preparing options for

27 *Report from the Commission to the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions – Progress of the EU's Integrated Maritime Policy*, COM(2012) 491 final, 11.9.2012, pp. 20-21.

28 *Maritime Surveillance in Support of ESDP. The Wise Pen Team Report to EDA Steering Board*, 26 April 2010.

29 *Maritime Surveillance in Support of ESDP. The Wise Pen Team Progress Report*, 22 October 2010.

the possible elaboration of a Security Strategy for the global maritime domain (..)."[30] The vague language of the conclusion reflected the battle that had started between the Commission and the European External Action Service about who would have the prime responsibility for drafting an EU Maritime Security Strategy. That battle of competences would slow down the follow-on work. By the autumn of 2013, more than three years after the Council's tasking, the EU Maritime Security Strategy was still lacking.

Main policies and instruments

CISE

As a follow-up to the IMP, in 2009 the Commission started its work on the establishment of a *Common Information Sharing Environment* (CISE) for the EU maritime domain. Four guiding principles for CISE development were established: interlinking all communities, across national boundaries and across sectors; building a technical framework for information exchange, taking into account data protection needs; the need to incorporate both civilian and military authorities in support of each other; and the requirement of specific legal provisions to remove obstacles for the exchange of data at the EU and national levels.[31]

In 2010 the CISE roadmap was adopted. It underlined the principle of "sharing on a need-to-know and responsibility-to-share basis" for data exchange.[32] This is very close to the wording of the Wise Pen Team. In the spring of 2011 the Council supported the roadmap and the CISE development "built on a decentralised information exchange framework interlinking relevant user communities (..)."[33] With this wording the Council confirmed that CISE should not lead to a completely newly built structure but rather result in a network connecting already existing networks. The Ministerial Limassol Declaration of 2012, which focused on underlining the importance of the EU's maritime dimension for jobs,

30 *Council conclusions on Maritime security strategy*, 3009th Foreign Affairs Council meeting, Luxembourg, 26 April 2010.

31 *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions – Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain*, COM(2009)538 final, 15.10.2009.

32 *Communication from the Commission to the Council and the European Parliament on a Draft Roadmap towards establishing the Common Information Sharing Environment for the surveillance of the EU maritime domain*, COM(2010)584 final, 20.10.2010.

33 *Council conclusions on integration of Maritime Surveillance – Towards the integration of maritime surveillance: A common information sharing environment for the EU maritime domain*, 3092nd General Affairs Council meeting, 23 May 2011.

economic growth and innovation (*blue growth*), supported the CISE development to become operational by 2020.[34]

The Commission also initiated two pilot projects for maritime surveillance to support the CISE development. These pilot projects were executed by different groups of member states. The MARSUNO project – Maritime Surveillance North – was launched in early 2010 and carried out by the EU Baltic Sea countries. The BlueMassMed (Blue Maritime Surveillance System Mediterranean), also started in early 2010, brought together 37 agencies responsible for maritime surveillance in six EU member states bordering the Mediterranean and its Atlantic approaches: Greece, Italy, Malta, France, Spain and Portugal. Both pilots produced useful lessons learned.[35] In 2013 the Commission launched a public consultation in order to collect the views of maritime and marine sector private stakeholders, citizens, non-governmental organisations and public authorities on CISE implementation.

EMSA

The European Maritime Safety Agency (EMSA) was established in 2003 to assist the member states and the European Commission with the development and implementation of EU maritime safety and pollution prevention rules. EMSA, based in Lisbon, has also been given operational tasks in the field of oil pollution response and with regard to the identification and tracking of vessels. The result is a European network called SeaSafeNet which is managed by EMSA. It links together a large number of maritime authorities. The information on vessel movements is gathered from coastal stations, able to pick up signals from vessels equipped with Automatic Identification System (AIS) responders, and port authorities all over Europe. In 2012 there were over 3,000 registered users of SeaSafeNet and more than 6 million ship position reports were exchanged per day.[36]

For vessel tracking beyond Europe's immediate surrounding waters the International Maritime Organisation (IMO) has set up a Long Range Identification and Tracking (LRIT) system. EMSA has set up a European component, the EU LRIT Data Centre which became operational in mid 2009. This centre also makes use of satellite information. For this reason EMSA has a great

34 *Declaration of the European Ministers responsible for the Integrated Maritime Policy and the European Commission, on a Marine and Maritime Agenda for growth and jobs - the 'Limassol Declaration'*, 8 October 2012.

35 See: *Final Report – MARSUNO* and *BlueMassMed Final Report*, www.ec.europa.eu.

36 Data and other details on EMSA are based on the *European Maritime Safety Agency – Annual Report 2012* and other EMSA information sources. See: www.emsa.europa.eu.

interest in the EU satellite programmes Galileo and GMES.[37] Both will serve to increase the accuracy and timeliness of data on ship movements, pollution or incidents at sea. The EU LRIT Data Centre is the biggest data centre of the whole LRIT system, tracking around 10,000 ships which generate a minimum of 40,000 position reports per day.

The third component of EMSA's vessel traffic monitoring is Thetis, the information system for port state control. It provides port authorities with the necessary targeting elements to select ships for inspection. EMSA is working on integrating all components into an Integrated Maritime Data Environment (IMDATE). A first prototype was tested last year. Another EMSA activity is CleanSeaNet, an oil slick detection system based on satellite surveillance and, when required, backed up by using other surveillance assets such as on-the-spot checks with patrol vessels or maritime patrol aircraft of member states. EMSA also contributes to Eurosur, the EU network for sharing data related to the border control activities of Frontex (see Chapter 3 for more detail).

In ten years' time EMSA has become a major provider of maritime data for the European Union and its member states. Its information is not only valuable to its traditional user communities (environmental control, transport and port authorities) but also to clients like Frontex using the available data for its border control activities at sea. Even the military are using EMSA data, namely for the EU's anti-piracy Operation Atalanta. Especially for this military operation EMSA has developed the Marsurv-1 integrated maritime data service. Based on the operational requirements of the military command of the operation Marsurv-1 links the information collected by EMSA's tools with other information provided by military intelligence sources to produce an enhanced maritime picture. Clearly, this improved maritime situational awareness picture helps the military to carry out their anti-piracy operation with more accuracy and increased effectiveness. But one should be aware that the sharing of information between EMSA and the military is case-specific. The existing rules do not allow EMSA to share data systematically with the naval authorities of the EU member states. Neither does EMSA receive data from European navies. In other words, the barrier to sharing civilian and military-generated information for maritime surveillance at the EU level continues to exist.

37 GMES = Global Monitoring for Environment and Security. The GMES programme aims at optimising the use of satellite Earth observation capacities for civilian users. It is also known as the Copernicus project. Galileo is the EU's satellite system for global positioning, the European variant to the American GPS. Both GMES and Galileo can also be used for military purposes.

EDA and other initiatives

The EDA has developed a maritime surveillance network, based on a common staff target agreed in 2008. In the summer of 2011 six EU coastal member states (Finland, France, Italy, Spain, Sweden and the UK) tested the 'Marsur network system', connecting existing naval and civilian data centres in these countries. In October 2012 twelve EU countries plus Norway signed a contract to further develop the technical elements necessary to use the Marsur network in a fully operational context. It will also allow for a secure network for the exchange of classified information in the support of CSDP operations. The programme should be fully operational by 2014.[38] Other examples of regional solutions are Sea Surveillance Co-operation Baltic Sea (SUCBAS) and the Virtual Regional Maritime Traffic-Centre (VRMTC) which connects 29 countries for regional monitoring in the Mediterranean and the Black Sea. The Maritime Safety and Security Information System (MSSIS) has been developed by the United States for operations in the Mediterranean. It is based on open sources data sharing (predominantly AIS based).

There are numerous activities related to maritime surveillance carried out by the European Commission, EMSA, EDA and different groups of member states. Old barriers, separating civilian and military data networks, have been lifted in practical pilot projects and even in real-life situations (EMSA-Operation Atalanta). The added value of connecting civilian and military data exchange systems to improve maritime surveillance has already been proven. The challenge is to bring them all together in one network of networks, which is not primarily a technical issue but requires above all legal and regulatory measures to be taken at the Brussels level.

National approaches

Maritime security is not a new topic for Europe's seaborne countries. Many EU member states have national strategies, policies and instruments to deal with the risks and challenges at sea. A closer look at three countries – Germany, the Netherlands and the UK – will reveal that there are important differences in national approaches to maritime security.

Germany

Although Germany is very dependent on the seas for its economic and social welfare the country lacks a maritime security strategy. In 2011 the German

38 Information from the EDA website (www.eda.europa.eu).

Federal Government adopted a 'Maritime Development Plan'.[39] Its section on maritime safety and security refers to security threats like illegal arms smuggling, piracy and human trafficking – which can affect all maritime players. The Plan strongly argues for internationally concerted and coordinated action. It also argues for national steering and coordination structures under the lead of the Transport Ministry, attempting to integrate all maritime actors in Germany. However, it does not address the consequences of maritime security risks and challenges for the integration of Germany's civil and military capacities. It says very little about the role of the German Navy in maritime security matters. The Plan has been written first and foremost from the perspective of the Federal Transport Ministry and driven by its need to establish an umbrella over all the maritime safety and security actors in the country.

The Defence Ministry's documents[40] depict the German Navy's role predominantly as expeditionary in order to deal with crises at their region of origin. The link between the country's broader maritime security interests and the navy's role is missing. The reason for this is that the German strategic mindset is very much land-based. According to a recent study, the defence documents contain "superficially discussed topics of maritime security" which "do not correspond with the economic and security-political priorities for Germany."[41] The same study concludes that the German Navy has sufficient capabilities for expeditionary operations, but that its capacities as a 'constabulary navy' should be expanded.[42]

Another particular German feature is the clash of competences between the German Federal Government and the coastal States (*Länder*). The latter are responsible for police tasks within German territorial waters, while the federal police is responsible for law enforcement within the Exclusive Economic Zone. In addition, several agencies bear responsibilities for maritime safety and security in their own areas, such as the customs office and the Central Command for Maritime Emergencies. It is "due to the unwillingness of government ministries and agencies to give up areas of jurisdiction" that Germany has not been able to

39 *Maritime Development Plan – Strategy for an integrated German maritime policy*, Federal Ministry of Transport, Building and Urban Development, 2011.

40 *White Paper 2006 on German Security Policy and the Future of the Bundeswehr* and the *Defence Policy Guidelines* (see footnote 9).

41 Prof.Dr. Carlo Masala and Konstantinos Tsetsos, M.A., 'The Maritime Dimension of the European Union's and Germany's Security and Defence Policy in the 21st Century – Maritime Security of the European Union (MAREU)', *ISPSW Strategy Series: Focus on Defense and International Security*, issue No. 229, May 2013, p. 16.

42 Ibidem, p. 39.

create a national coast guard.[43] Instead a Maritime Safety and Security Centre - MSSC (*Maritimes Sicherheitszentrum*) has been established in Cuxhaven to coordinate between all responsible actors dealing with maritime security. Its operational core – the Joint Maritime Emergency Reporting and Assessment Centre (MERAC) – acts as the communication hub. It guarantees an integrated exchange of information between all services and is responsible for the coordination of all operational means. While all civil maritime security actors are integrated into the MSCC, the German Navy only has a liaison element at the Centre.

The German case shows that the separation of responsibilities (Federal and coastal State levels) and operational tasks (civilian security agencies and the navy) is difficult to overcome. The German example also points to the impact of geography and history on the country's security policies and structures. Despite the importance of sea trade for its economy and an impressive naval history Germany remains a primarily continentally-oriented European country. The unification has reinforced its central role in *Mitteleuropa*. Berlin's attitude to the deployment of military means for international crisis management has changed quite substantially since the early nineties, but the country remains reluctant to use 'hard power' in dealing with security problems. These factors certainly help to explain why Germany has no maritime security strategy and is lacking a civil-military integrated apparatus to deal with the new security risks and challenges at sea.

The Netherlands

In the Netherlands the Ministry of Infrastructure and the Environment is responsible for maritime affairs. Its website provides zero information on maritime security. The section on "water and security" basically deals with water management issues related to risks like flooding or storms and maritime safety. The Dutch National Security Strategy pays no particular attention to maritime security.[44]

The only authority which has addressed maritime security publicly is the Royal Netherlands (RNL) Navy. The 'Maritime Vision 2030', published in 2009 and building on earlier documents, describes a 'future maritime dimension' which takes into account elements like the impact of climate change and energy policies, the quest for maritime natural resources, the risks and challenges posed by crime and terrorism at sea and other security developments. Thus, the RNL Navy clearly recognises the vanishing distinction between external and internal

43 Ibidem, p. 21.
44 See chapter 1.

security. This future maritime dimension has important consequences for the missions and tasks of the RNL Navy. National tasks in support of the civilian security authorities are becoming even more important. The North Sea is one of the busiest sea areas in the world. This will further increase: "Thus, it is essential that in 2030 a completely integrated, military and civilian maritime situational picture of the North Sea will be continuously available and that sufficient interception means will be on stand-by."[45]

The Dutch Coastguard in its current set-up became operational in 1987. It is a civil organisation, but embedded into the RNL Navy. The Coast Guard Centre is located at the Naval Base in Den Helder. The Director of the Coastguard is always a naval commander. Vessels and air assets are owned by the various ministries and services. Maritime situational awareness is created by fusing information from AIS, radar and air surveillance and by identifying potential risks by combining all information sources of the Dutch Government, including of the law enforcement agencies (the police, customs, the immigration service, the food & safety authority, etc.). All participating ministries signed the underlying information-sharing protocol. This approach is unique in the EU. In the Netherlands the legal barrier to sharing information between the different agencies has been overcome.

The Dutch example shows that the navy can significantly contribute to maritime security, not only during operations far away from its home base but also in a supporting role to the Coastguard in waters close to European territory. They are natural partners. Without an integrated maritime security strategy or policy the Dutch have pragmatically organised an effective approach to dealing with maritime security.

The RNL Navy is also providing means and assets to other ministries and agencies, such as navy divers for port security activities. Naturally, there is an inherent interest in the RNL Navy in maintaining and broadening these activities in the fight for budget allocation in times of austerity. But this orientation on non-traditional, non-military risks and challenges can also be explained by the long tradition of the Dutch navy in protecting the political, economic and social interests of the country dating back to the 16-17th century when the Republic rose to world power status due to dominating the seas. Ever since the Golden Age the RNL Navy has had a broad orientation, not only based on fighting wars and crisis management tasks but also related to the Dutch political and economic interests in keeping the world's sea lanes and passages open and free from conflict.

45 *Maritieme Visie. De Koninklijke marine in 2020 Voor veiligheid op en vanuit zee*, maart 2009. All quotes translated into English by the authors.

United Kingdom

It comes as no surprise that the United Kingdom pays particular attention to maritime security. The country is highly dependent on the seas in nearly every aspect of its interests, from economic prosperity and the welfare of the British population to London's influence on international affairs. Consequently, the UK has cross-government policies and structures in place for maritime security. The Home Office has overall responsibility for all relevant maritime activity related to law enforcement activities such as immigration, border control, countering drugs trafficking and terrorism. The police, the UK Border Agency, the security service (MI5) and other organisations bear specific sector responsibilities. The Department for Transport (DfT) is responsible for the 'UK national maritime security programme' which covers all commercial maritime operations and activities.[46] The Royal Navy is a key stakeholder in supporting the agencies responsible for the integrity of UK waters "including protection of offshore installations, shipping routes, anchorages and the fishing fleet" and it conducts inter alia "drug interdiction, anti-pollution enforcement and provides platforms to the Security Service and the Secret Intelligence Service when required."[47] The role of the Royal Navy for the protection of offshore platforms is likely to increase as "naval hardware is developing rapidly to meet the new threats using automatic, wide-area, remote sensing systems."[48]

There are two coordinating bodies. The National Maritime Information Centre (NMIC) is a cross-government organisation located at the military Northwood Headquarters near London. It became operational in April 2011. NMIC acts as an information distribution centre. The Maritime and Coastguard Agency (MCA) is the executive branch of the DfT. MCA coordinates search and rescue at sea and it monitors and checks the application of maritime safety standards. It also has a command and control task in case of maritime shipping incidents which could cause pollution in UK waters.

The MCA's role will become more important with a modernised maritime surveillance system which should be ready by 2015. It will be coordinated and managed from a new Maritime Operations Centre in Southampton.[49] However, there is great concern about the long-range maritime surveillance picture since the UK Ministry of Defence decided in the 2010 Strategic Defence and Security Review (SDSR) to scrap the modernisation of the Royal Navy's maritime patrol aircraft (the Nimrod MRA4 programme) for which already 3.2 billion pounds

46 *Brief overview of the UK national maritime security programme*, www.gov.uk.

47 *UK Marine Security Market Report – The Canadian Trade Commissioner Service*, 8th March 2013, p. 14.

48 Ibidem, p. 46.

49 Ibidem, pp. 20 + 45.

had been invested. In its report on maritime surveillance of September 2012 the House of Commons Defence Committee expressed its worries about the loss of this capacity which it considers of strategic importance for protecting the UK's interests and commitments both in the military and non-military arenas.[50] The Secretary of Defence has already announced that the next SDSR (2015) will include a decision to fill the capability gap on maritime patrol aircraft. The Committee warns against an isolated defence decision and recommends "that work on the next SDSR should include a specific maritime surveillance work stream, involving all those, military and non-military, who make use of these assets." The concern about cross-government cooperation is not only related to long-range maritime surveillance. The Defence Committee's report shows that there are still shortcomings in cross-sector coordination and in some cases an overlap of assets.

The British case shows that the more actors that are involved the more difficult it becomes to establish well-functioning coordination mechanisms between all civil and military actors involved in maritime security. There is still a considerable overlap of operational responsibilities and tasks, not in the least as a result of unfinished turf battles. Decisions on capabilities, such as for long-range maritime surveillance assets, have been taken by the Ministry of Defence in too much isolation from the other departments. A civil-military integrated coastguard with full responsibilities does not exist in the UK. The result is a mix of authorities, agencies and coordination bodies which seems to lack an effective overall umbrella structure which can steer all these actors to create maximum efficiency and effectiveness.

The way forward

The three case studies deliver a picture of various national approaches to maritime security. In a nutshell and in black and white terms: Germany has neither a strategy nor a civil-military integrated system; the Netherlands has no strategy but operates with an integrated civil-military apparatus; and the UK has a strategic programme for civil-military integration but is struggling with its implementation. The cases also show that national history, geographic location, organisational culture and bureaucratic obstacles impact heavily on a country's maritime security policy and structures. Therefore, it is difficult to deduct general conclusions from the case studies for an EU maritime security strategy and in particular for related organisational models. On the other hand, EU member states might relatively easily agree on defining the maritime security environment

50 *Future Maritime Surveillance*, House of Commons Defence Committee, Fifth Report of Session 2012-2013, HC 110, 19 September 2012.

which is characterised by a wide range of risks and challenges to a broad set of interests. All three case studies do show that nations see maritime security as vital to national political, economic, social and environmental well-being. In other words, maritime security is much more than safeguarding security at sea through military power. It requires the involvement of many ministries from Foreign Affairs and Defence to Justice and Home Affairs, Transport, Fisheries and the Environment. Equally a broad pallet of instruments, civilian and military, is needed to deal with security challenges varying from piracy and mines to illegal immigration, pollution, drugs trafficking and other criminal acts.

Maritime security can only be seen as a mixture of external and internal security elements which requires a civilian-military coordinated or integrated response. In her final report preparing for the December 2013 European Council High Representative Catherine Ashton makes the plea for "a strategic, coherent, functional and cost-effective approach to maritime security."[51]
The EU maritime security strategy will have to encompass at least the following elements: its application has to be global; its approach has to be civil-military; its participation has to be comprehensive, involving all actors across the traditional external-internal security divide; its governance should be based on legal responsibilities, with the appropriate authority for member states in their coastal waters and exclusive economic zones; its structure has to be integrated to the extent possible in terms of operational instruments, civil and military; its capabilities will require planning coordination between all ministries involved and at the EU level between the CSDP, maritime policy and internal security actors, including the relevant EU agencies.

The real challenge will be to translate this set of requirements into the optimal structures involving civilian and military actors. Maritime surveillance stands out as the capacity which seems to have advanced the furthest in the direction of a civil-military integrated approach. What is needed is to stop the proliferation of pilot schemes, projects, regional and other solutions and to bring them all together in a European-wide network of networks. The European Commission's CISE should provide the umbrella network but, naturally, theory needs practical implementation. EMSA is the only agency with Europe-wide coverage. Thus, this Lisbon-based agency is in the ideal position to provide the operational leg of CISE, the practical network of networks. However, this requires a fundamental change. At the Brussels level the legal barriers of non-cooperation with the military will have to be slashed and internal turf battles between different parts of the European Commission have to be overcome. For civil-military data exchange, EMSA's assistance to Operation Atalanta has already proven that it is

51 Final Report by the High Representative (see footnote 21).

practically feasible. Now, the statute of EMSA should by amended to allow for structural cooperation with the military, both at the EU level and with the member states' navies. That also requires European navies to share their data with EMSA. Civil-military maritime surveillance information exchange has to be a true two-way street.

Civil-military integration should not be limited to information exchange. Many navies have been involved in anti-immigration and counter-drugs operations for years, both in European waters and elsewhere such as in the Caribbean. Frontex will continue to call on the member states to assist the agency with military assets, such as patrol boats and aircraft. Increasingly, civilian and military capabilities overlap in their use, in their technical requirements and even in their funding. Pooling and sharing should not be limited to Europe's military but has to be extended to combining civil-military means and assets. Maritime patrol aircraft can be brought together in a European civil-military common pool, from which capabilities in excess of national needs can be made available to other states in need of long-range maritime surveillance aircraft. For the more distant future the acquisition of maritime patrol aircraft can be combined between member states' civilian and military planning authorities, perhaps to start in smaller clusters for the Baltic Sea, the North Sea, the Atlantic approaches and the Mediterranean. The same could apply to remotely piloted aircraft systems (RPAS). Coastguard vessels and navy patrol boats can be pooled in the same manner. In many cases search & rescue organisations are already based on combining civilian and military means. Countries can build on this experience and widen the integration to medical and other services. There is also a huge potential for combining the training of civilian and military personnel, nationally, regionally and ultimately at the EU level. Exercises involving civilian and military actors, so far predominantly held at the national level, should be internationalised once maritime security-related cross-border cooperation starts to increase.

For an integrated EU maritime security strategy to see the light of day in the near future, its implementation calls for a step-by-step approach of various building blocks – data sharing, combining assets, planning of capabilities, training and exercises. The exchange of maritime surveillance information should be enhanced by connecting national and regional systems to an EU network of networks operated by EMSA. For arranging other civil-military capacities bilateral or regional clusters are more likely to succeed in the foreseeable future than EU-wide structures. At the European Union level this should be recognised and supported in the interest of moving towards an overall EU maritime security regime.

3 Case study border security

Growing importance of border control

The EU has 11,000 kilometres of external land borders, 43,000 kilometres of external sea borders[52] and 286 international airports. Border security is a major challenge for the Union and these facts underline the necessity to make border security a common task.[53]

There is an uneven distribution of burdens between EU member states to deal with increased pressures on the external borders. Countries along the southern borders – Italy, Spain, Malta, Cyprus, Bulgaria and Greece – are especially vulnerable to border security breaches.[54] This became particularly acute with the fallout from the Arab Spring causing a rise in immigrants and refugees heading for Europe. In 2011 a sharp rise (to more than 40,000) in the number of people crossing illegally was detected, particularly at the Mediterranean sea borders and the Greek-Turkish land border. The number dropped to below 14,000 illegal crossings at the end of 2012.

Italian authorities have reported that 35,085 migrants landed on Italian coasts since the beginning of 2013. Some 25,000 of these had been rescued at sea. Tragically, several boats capsised, resulting in the loss of hundreds of illegal immigrants. By mid-October the situation south of Sicily had turned into an emergency, which required wider involvement of the Italian Navy. On 18 October Italy launched Operation Mare Nostrum. The Italian Navy, which was already contributing to maritime surveillance and search and rescue operations, stepped up its efforts. Under Mare Nostrum it has deployed six ships, helicopters with infrared equipment and maritime patrol aircraft. The Italian Air Force is contributing with Predator B unmanned drones. According to Italian government representatives the national operation would be integrated with the wider EU Frontex and Eurosur maritime security activities.[55] On 24-25 October the European Council called for reinforcement of the Frontex activities and established a Task Force for the Mediterranean which should identify "priority actions

52 The Schengen area has 42,672 kilometres of external sea borders. The total length of the EU's coast line is approximately 90,000 kilometres (see Chapter 2).

53 *Frontex: cooperation with countries outside the EU*, Warsaw: Frontex. See: www.euromed-migration.eu.

54 Michela Ceccorulli, *Migration as a security threat: internal and external dynamics in the European Union*. GARNET Working Paper No. 65/09, Florence, April 2009.

55 *Italy to strengthen maritime presence for Mediterranean migration crisis*, Jane's Defence Weekly, 16 October 2013; *Mare Nostrum Launched by Italy*, ANSAmed, 16 October 2013.

for more efficient short term use of European policies and tools". The European Council should take operational decisions in December 2013.[56]
It comes as no surprise that High Representative Catherine Ashton has described border security as an integral part of the EU's security in her final report for the December 2013 European Council.[57] She argues that the EU should use a variety of suitable instruments at its disposal, including CSDP missions, the European Neighbourhood and Partnership Instrument, Frontex, the Instrument for Stability as well as other EU external cooperation instruments.

Main policies and instruments

The Amsterdam Treaty of 1999 formalised the creation of an 'Area of Freedom, Security and Justice' (AFSJ) and officially incorporated the Schengen acquis in the EU's legal framework.[58] With increased freedom within the borders of the EU, so-called 'compensatory measures' were introduced to safeguard internal security. This involved improving cooperation and coordination between the police and the judicial authorities in order to safeguard internal security and, in particular, to fight organised crime.
Over the years the European Union has launched a series of programmes and initiatives in support of the AFSJ.[59] After the Lisbon Treaty came into force the competences of the Commission in the area of AFSJ has been strengthened, although the JHA Council also has the power to "define the strategic guidelines" (art.68 TFEU). For all substantive AFSJ legislation, Commission proposals are subject to the ordinary legislative procedure: a co-decision between the European Parliament and the Council, which acts by a qualified majority. In terms of substance within AFSJ, the Commission mostly seems to lean towards safeguarding the fundamental rights and freedoms of individuals, while the JHA Council puts more emphasis on the importance of security and enforcement measures.

Frontex

Frontex is the key institution for managing the EU's external borders. It was created by a Council decision of 26 October 2004 with the main objective of coordinating operational cooperation amongst member states to strengthen security at the external borders of the EU member states.[60] The agency officially

56 *Conclusions European Council*, Brussels, 25 October 2013, EUCO 169/13.
57 *Final Report by the High Representative* (see footnote 21).
58 The Schengen zone with a single, common border encompasses 26 European countries.
59 Including the 1999 Tampere Programme, the 2004 Hague Programme on strengthening freedom, security and justice in the EU and the 2009 Stockholm programme.
60 Data on Frontex can be found at www.frontex.europa.eu.

became operational on 1 May 2005 and is based in Warsaw, Poland. Frontex's financial resources have increased significantly (from € 6 million in 2005 to € 86 million in 2011). At the end of September 2011, Frontex's budget for 2011 was increased for an Emergency Response Package in the Mediterranean to help combat growing migration problems. This has brought the total operating budget for 2011 to €118 million.[61]

Most of Frontex's budget is spent on the coordination of joint operations at the external borders of the EU (almost 50%). Frontex has the competence to coordinate joint operations at external air (airports), land and sea (seaports) borders. These operations can be proposed by member states or initiated by the agency itself.[62]
While regular border control is the exclusive responsibility of the member states, Frontex's role focuses on coordinating the deployment of additional teams of experts and technical equipment to those border areas which find themselves under significant pressure. It is important to note that Frontex does not have its own border guards, but relies on member states to second these to participate in Frontex operations. While performing their tasks and exercising their powers, members of these Frontex teams may carry service weapons, ammunition and equipment as authorised according to the national law of the sending member state. However, the host member state may prohibit the carrying of certain service weapons, ammunition and equipment, provided that its own legislation applies the same prohibition to its own border guards. All actions by a Frontex-coordinated operation occur, as a general rule, in the presence of border guards of the host member state. The host state's command officer has operational responsibility for the team and has the authority to give instructions to his assigned team.[63]

The Frontex Situation Centre in Warsaw which gathers and collates information from partner countries, within and beyond the EU's borders, as well as from open sources such as academic publications and the press, in order to monitor the day-to-day situation at the EU's external borders. Member states provide Frontex with information on illegal border crossings, illegal stays, refusals of entry, asylum applications, facilitation, false documents and returns of illegal stayers.

61 *Frontex, General Report 2011*, Warsaw. See: www.europarl.europa.eu.
62 Article 3 of EU Regulation (EC) No. 2007/2004.
63 *Parliamentary Oversight of Security and Intelligence Agencies in the EU*, European Parliament, Directorate-General for Internal Policies, Brussels, 2011.

Frontex has been heavily criticised since the start of its operations in 2005, particularly by human rights groups. For instance, the 'push-back' operations during which refugee vessels are being intercepted and escorted back to their ports of origin are vulnerable to criticism. Although no reliable statistics exist on the number of fatalities at sea, civil society organisations have tried to estimate the size of the tragedy by using indirect sources, such as incidents reported in the press and accounts provided by eyewitnesses. 2011 recorded the largest number of migrant deaths in the Mediterranean since 1994: by early December, 2,251 migrants had died or gone missing in the Sicily Channel alone.[64]

The legal basis of Frontex was last amended by a Regulation of the European Parliament and of the Council of 25 October 2011.[65] Notable is that the operational maneuverability of Frontex has been made more precise and has widened. One of the changes is the further development of the resources pools of Frontex for personnel and equipment. Until 2011 the operational teams of Frontex were called Rapid Border Intervention Teams or RABITs. They are now renamed as European Border Guard Teams (EBGT). The pool of the EBGT now consists of 1,850 border guards seconded by the member states. A number of them are earmarked for rapid intervention operations. Once member states have concluded their yearly agreement with Frontex on their contribution to this EGBT pool, they have a legal obligation to make their border guards available for deployment at the request of Frontex, unless they are faced with an exceptional situation substantially affecting the discharge of national tasks. This arrangement is more compulsory than that of the previous regulation. Frontex now works on the development of a Frontex secondment system, having created the status of 'Seconded Guest Officer' (SGO) in 2012. The SGO status allows Frontex to have seconded personnel deployed for six months and not for the customary one-month secondment period. This has obvious efficiency and cost-savings advantages, but it does require sending member states to weave this into their personnel and recruitment systems to ensure that these types of secondments remain workable and attractive for their personnel.

The Frontex equipment pool has also been renamed with the 2011 Amended Regulation. In 2011 the Central Record of Available Technical Equipment (CRATE) was renamed the Technical Equipment Pool (TEP), which lists items

64 *Fundamental Rights: challenges and achievements in 2011, Annual Report 2011*, European Union Agency for Fundamental Rights, Luxembourg, 2012, p. 74.

65 *Regulation (EU) No. 1168/2011 of the European Parliament and of the Council of 25 October 2011 amending Council Regulation (EC) No. 2007/2004 establishing a European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union*. See: www.frontex.europa.eu.

of surveillance and control equipment that member states are temporarily willing to put at the disposal of another member state for Frontex operations.[66] In its yearly risk assessment, Frontex determines the minimum number per type of technical equipment. Since migration flows are volatile, yearly planning is necessary. As with the EBGT the equipment pool has the same provisions which require member states to stick to the agreement they have concluded with Frontex and make their technical equipment available upon request. Financial regulations to pay for the deployment of the equipment are in place.
The yearly planning of the TEP complicates cooperation with the defence sector. Defence ministries tend to plan ahead for more than one year. In addition, with the current downsizing of armed forces and lower levels of ambition, also the capabilities needed for participation in Frontex border security operations need to be made part of the level of ambition for deployments. According to one source, at the beginning of 2010 assets offered by 21 member states comprised 21 fixed-wing aircraft, 27 helicopters, 116 vessels, mobile radar units and other specialised technical equipment such as forgery detection kits, ultra-violet lights or heartbeat detectors.[67] One official mentioned that Frontex will be needing (among other things) approximately 80 ships in 2014. Lists of the content of the TEP or of contributors are not in the public domain.
Article 7 of the Amended Regulation also stipulated that Frontex is allowed to acquire technical equipment itself. In addition, it may lease or buy equipment in co-ownership with member states. The 2011 Regulation mentions examples of major technical equipment which Frontex could acquire: "open sea and coastal patrol vessels or vehicles" (Art. 7.1). In 2013 Frontex has launched a pilot project for leasing equipment.[68]

A legal problem with EU agencies such as Frontex owning equipment, for example vessels, is the flag issue. Ships can only sail under the flags of states and although the EU has legal personality, it is questionable whether it is possible under international maritime law for it to function as a flag state. It is probably for this reason that the possibility of co-ownership between Frontex and the member states is written into the Amended Regulation. Article 7.1(a) stipulates that in the case of acquisition and co-ownership, the member state "will provide for the registration of equipment in accordance with the applicable legislation of that Member State". The next subsection of Article 7 then provides for a "model agreement" in which modalities will be agreed "ensuring the periods of full availability of the co-owned assets for the Agency". It seems that the 2011

66 Sarah Léonard, 'EU border security and migration into the European Union: FRONTEX and securitisation through practices', *European Security*, 19:2, 2010, p. 239.
67 *Frontex Executive Director invited to France*. See: www.frontex.europa.eu.
68 *Frontex General Report 2012*, Warsaw. See: www.frontex.europa.eu.

Frontex Regulation can be regarded as a model for how the EU could provide other EU security sectors (including defence) with dual-use assets.

The 2011 amendments do not end Frontex's development. Recently, the European Commission has begun a study which investigates whether the EU needs its own European border guard organisation. In October 2013, Frontex held a conference to consider what the future of the European border security in 2025 might be. Moreover, the escalation of illegal immigration near Lampedusa and Malta in the autumn of 2013 has also led to a widening of Frontex's remit and the scope of its operations in the Mediterranean.

One of Frontex's core tasks is to serve as a platform to bring together Europe's border-control personnel and the world of research and industry to bridge the gap between technological advancement and the needs of border control authorities. At the core of Frontex's research and development (R&D) work is an exploration of the potential offered by new border management technologies.[69] The development of these technologies is funded through various budget lines: the EU External Borders Fund, the framework research programmes (Horizon 2020) and the Internal Security Fund. Apart from these considerable resources attributed to border control research and development, the Development Cooperation Initiative is used when non-EU third country measures are concerned.[70] The increasing funding for border control can also be detected in the 'security' part of the Multi-annual Financial Framework (MFF) 2014-2020 of the Union budget. Some 26.8% is attributed to security challenges of which border security is an important part. In comparison, the budget line 'global Europe' (among which is CFSP) has risen by only 3.3%.[71] It is estimated that under the Horizon 2020 programme € 3,819 billion will go towards security research under the heading "inclusive, innovative and secure societies".

Eurosur

Among the border control initiatives, the European External Borders Surveillance System (Eurosur) is the most comprehensive. Frontex describes it on its website as "the backbone of European border surveillance". The purpose of Eurosur is to improve the situational awareness and reaction capability of member states and Frontex when preventing irregular migration and cross-border crime at the external land and maritime borders, particularly

69 *Role*. See: www.frontex.europa.eu.

70 Ben Hayes and Matthias Vermeulen, *Borderline. The EU's New Border Surveillance Initiatives*, Heinrich Böll Stiftung, June 2012, p. 68-69.

71 Patrik Pawlak and Erik Brattberg, *Equipping the EU for future security challenges through strategic planning*, UI Occasional Paper, no. 20, June 2013, p. 11.

the southern maritime and eastern land borders.[72] This aim should be realised by (i) interlinking 24 different national surveillance systems and National Coordination Centres (NCCs), bilaterally and through Frontex[73], (ii) making optimal use already existing EU capabilities and information networks, and (iii) by potential use of new capacities such as satellite observation (GMES), drones and autonomous targeting systems. Remotely piloted aircraft systems are getting special attention for providing enhanced surveillance coverage of long stretches of land and sea borders. This is of particular importance in improving search and rescue success rates. Planned activities in this respect include further research on the deployment of RPAS for European border surveillance, and organising practical demonstrations and tests of the equipment. At the moment, Frontex faces similar challenges as other (potential) users of RPAS (such as defence) and struggles with the cost-effectiveness of RPAS and integration into normal airspace. Cooperation with EDA, which has already undertaken a study on Spectrum requirement for military UAS Insertion in General Air Traffic (SIGAT), could provide interesting synergies. Currently, 15 projects related to border security are funded by EU security research funds of which two have specific bearing on RPAS and seven are related to GMES.[74]

By 2015 Eurosur should enable the national coordination centres to exchange information with other communities with interests in the EU maritime domain, such as transport, fisheries, customs and defence.[75] Eurosur should become operational in early December 2013. In the framework of a so-called Big Pilot the first NCCs have been linked through a secure communications network. The remaining NCCs of the member states have been linked in 2012 and the last will follow in 2014. Official figures indicate that the development of Eurosur will cost € 338 million, but observers have estimated that the costs are much higher and go up to € 874 million.[76]

Frontex, Eurosur and CSDP

As the High Representative has indicated CSDP and border security are linked. However, there are several problems here. The exchange of information between the EU (Frontex) and the member states is a sensitive issue. While the Eurosur

72 *Proposal for a Regulation of the European Parliament and of the Council Establishing the European Border Surveillance System (EUROSUR)*, Brussels, 12 December 2011, COM(2011) 873 final, p. 2.
73 Hayes and Vermeulen (see footnote 70), p. 8.
74 An overview is provided by Hayes and Vermeulen (see footnote 70), pp. 60-66.
75 *Determining the technical and operational framework of the European Border Surveillance System (EUROSUR) and the actions to be taken for its establishment*, European Commission Staff Working Paper, p. 11.
76 Hayes and Vermeulen (see footnote 70), p 8.

system rests on already existing national or European instruments and tools, it is likely to create synergies that may have an impact on fundamental rights, especially in relation to asylum and data protection.[77] Various regulations and arrangements have been listed in the Eurosur proposal to specify how classified information is handled and who has access to which information.[78] This could complicate the dual-usage of Eurosur capabilities.
Only information with relevance to external border control is exchanged with Eurosur. A minimalist interpretation of this could block the possible military application of the information from the Eurosur framework and infrastructure by EU member states or CSDP structures. Particularly "maintaining a common pre-frontier intelligence picture"[79], which is de facto a monitoring of crisis-affected areas in the southern neighbourhood of the EU, can be of great use for CFSP and CSDP purposes, including for conflict management missions and operations. Frontex already has a role in facilitating CSDP border management missions, such as EUBAM Libya and EUBAM Moldova/Ukraine, but also rule of law missions such as EULEX Kosovo. In Libya, Frontex has been closely associated with the planning of the mission and will complement mission activities.[80]

CSDP missions and operations and Frontex can clearly be mutually reinforcing, but there is also a potential for contradictory policy goals, which necessitates a coordination of policies. An example is the case of the Frontex involvement in Kosovo, which has been aptly described as the dilemma between "gate-keeping and state building".[81] The EU should take a step back and look at the security objectives from various angles, ask the question 'security for whom?' and consider which policy tool can be used for what objective. A CSDP mission is ideally part of a comprehensive approach in which also the 'root causes' of conflicts are addressed, while Frontex activities are geared towards managing the effects of conflicts. Eventually, security for citizens in conflict-ridden countries can be equated with security for EU citizens, but various policies and instruments have to be applied carefully so as not to lose sight of European values and long-term consequences.

77 *Fundamental Rights: challenges and achievements in 2011* (see footnote 64), p. 74.
78 *Proposal for a Regulation* (see footnote 72), pp. 12-15.
79 Ibidem, p. 16.
80 *EU Border Assistance Mission in Lybia 2013*, European External Action Service. See: www.eeas.europa.eu.
81 Eva Gross, *Policy recommendations report on managing the changing relationship between CFSP/CDSP and the jurisdiction and activities of FRONTEX*, Deliverable submitted November 2010 (M32) in fulfillment of the requirements of the FP7 project, Converging and Conflicting Ethical Values in the Internal/External Security continuum in Europe (INEX), PRIO, p. 5. See: www.inexproject.eu.

Benefiting from the information generated through the Eurosur network is one of the advantages for member states' defence organisations and for the headquarters conducting CSDP operations. The Executive Director of Frontex, Ilkka Laitinen, is looking to expand its surveillance operations beyond the EU to develop a so-called "common pre-frontier intelligence picture [CPIP]". He said: "This is where Frontex is due to arrange the delivery and the production of additional surveillance data from an area that is beyond the border, typically we are talking about international borders or some further areas."[82] Another benefit would be that research and development on surveillance technology and networking between national systems could deliver hybrid civil-military standards which would allow usage for defence purposes. The defence interest for Eurosur could therefore be twofold: (1) to be part of the user community and (2) to obtain access to standards, infrastructure and research and development.

National approaches

The Netherlands

The Netherlands has been part of the Schengen agreement from its inception and is also a full participant in Frontex. The Netherlands only has European external sea borders, airports and seaports to manage. The Royal Netherlands Marechaussee (KMar)[83], a police force with military status, is responsible for these external borders, with the exception of the port of Rotterdam area, which is the jurisdiction of the regional Seaport Police. The Royal Marechaussee and the Royal Netherlands (RNL) Navy participate in the Coast Guard Centre located in Den Helder.[84]

The Dutch acknowledge that their interest in secure external EU borders is high and therefore the Netherlands is a relatively active participant in the Frontex organisation and operations. The Netherlands has a permanent pool of 200 personnel for the European Border Guard Teams of which 15 are on stand-by for rapid reaction operations. It is not only the Royal Marechaussee that contributes to the permanent EBGT pool. Approximately 120 are KMar, while the remaining 80 have a varied profile, such as interpreters, debriefers, dog handlers, Seaport Police, etcetera.
The Netherlands has a track record in assisting Frontex operations in Spain, Greece and off the Italian coast. For example, the RNL Navy contributed three mine hunters, a torpedo vessel and a staff element to Operation INDALO in 2011 to combat illegal immigration in the coastal areas of South-East Spain.

82 *Frontex chief looks beyond EU borders*, EU Observer, 14.01.13.
83 In Dutch: Koninklijke Marechaussee.
84 See chapter 2 for further details on the Dutch Coastguard.

The Netherlands also contributed substantially to the RABIT rapid intervention operations at the Greek-Turkish land border in 2010 and 2011 with in total 48 KMar officers and a number of interpreters. In 2013 a number of KMar officers assisted at various airports in the EU: Madrid, Stockholm, Rome, Bucharest and Milan.[85]
A complication is that the Royal Marechaussee is struggling with the fact that deploying their border guards with military status for six months to Frontex could in practice mean that the same persons are sent on a mission of the Ministry of Defence the moment they return to their jobs. This is caused by the fact that a Dutch Marechaussee performs tasks for two different Ministries: the Defence Ministry and that of Security and Justice.
The Netherlands is also participating in Eurosur and has appointed the Coast Guard Centre in Den Helder as the National Coordination Centre. The national information system used by the Seaport Police and the Royal Marechaussee, ZUIS (Shipping Extendable Information System),[86] can be linked to Eurosur. This is regarded as a clear added value of Eurosur.[87] The Netherlands also expects that by connecting information, the coastline and small ports and vessels, which were regarded as a hiatus in surveillance, can be surveyed more effectively.[88] Due to the phasing of the project, the Netherlands will be among the last member states to be connected in 2014.

At the moment, there is no structural and organised interest by other Dutch armed forces services in participating in the Eurosur project. However, on a more ad hoc basis, the Royal Netherlands Army has indicated interest in the technology used in Eurosur. The KMar is an organisation with its roots in the defence organisation and is exposed to civilian security technology and its applications. It could therefore be argued that the KMar has the responsibility to bring these worlds together for the benefit of the whole defence organisation.

United Kingdom

The management of borders has in recent years been a troublesome affair in the United Kingdom. In 2013 it was announced by the Home Secretary, Theresa May, that UK Border Agency (UKBA) – a large organisation with 25,000 staff – is to be abolished and brought back within the Home Office. The Agency is regarded to have four main problems: its size, its lack of transparency, its IT systems and its policy and legal framework. The UKBA will be split into

85 Information from the Dutch Government website www.rijksoverheid.nl.
86 In Dutch: Zeevaart Uitbreidbaar Informatie Systeem.
87 *Brief van de Staatssecretaris van Buitenlandse Zaken aan de Eerste Kamer*, 13 januari 2012, p. 9.
88 *Tweede Kamer der Staten-Generaal, EU-voorstel: verordening Oprichting Europees grensbewakingssysteem (Eurosur), Verslag van Algemeen Overleg*, 12 maart 2012.

an immigration and visa service and a separate law enforcement command while bringing it back under the direct control of the government.[89]
Already in May 2012, after a very critical report on the functioning of the UKBA, the Border Force was separated from the UKBA and has become a separate law enforcement operational command, led by its own Director General, and accountable directly to Ministers. A September 2013 National Audit Office report, however, was still very critical about the Border Force's ability to meet its objectives, particularly in the areas of sufficient staffing, efficiency and making optimal use of technology.[90] The Border Force patrols the UK coastline and carries out immigration and customs checks at ports and airports.[91] The Border Force has a fleet of five fast patrol ships, known as cutters. They protect the coastline non-stop and are the only national, non-military, maritime vessels for enforcement, surveillance, and stop-and-board activity that do this. They can be put into service within 30 minutes.

Three key characteristics of UK border security can be distinguished: the 'off shoring' of the border away from UK territory, the reliance on technologically advanced forms of identity management, and an increasingly pre-emptive logic based on risk profiling.[92] Key in the increasing reliance on technological means is the UK's e-Borders programme. This initiative, which involves data capture prior to travel and analysis undertaken at the new Joint e-Borders Operations Centre, aims to count foreign nationals entering and exiting the UK.

The UK is not part of Schengen and therefore contrary to the UK's wishes, is also not a participant in the Frontex Regulation. It is nevertheless able to be involved in the activities of Frontex on a case-by-case basis with the approval of the Frontex Management Board. In practice, this means that the UK is actively participating in numerous operations to which it contributes Border Force officials. London also contributes financially to operations in which the UK is involved. It regards participating in Frontex operations as very useful in terms of gaining experience in the border management practices of others and in gathering information. The UK border forms part of the external boundary of the European Union. It therefore operates European Union customs controls on goods entering or leaving Europe at the UK border.

89 'UK Border Agency to be Abolished, Theresa May announces', *The Guardian*, 26 March 2013.
90 *The Border Force. Securing the Border*, National Audit Office, 4 September 2013.
91 See Border Force website via www.gov.uk.
92 N. Vaughn-Williams, 'The UK Border Security Continuum: Virtual Biopolitics and the Simulation of the Sovereign Ban', *Environment and Planning D: Society and Space*, volume 28, April 2010, p. 1072.

The House of Commons expressed its concerns that the UK is not able to take part in the Eurosur project, which could mean less access to surveillance data, as it is not a part of the Schengen acquis. However, the Minister made clear that "there is nothing in the draft EUROSUR Regulation that specifically restricts Frontex from continuing to share its risk analysis products with existing customers (...) ".[93]

The way forward

EU border management will remain a clear growth area. The urgency of coordinating and sharing responsibility for the EU's external borders is reflected in a growing Frontex agency, increasing budgets available for border management in the EU's multi-annual financial framework and for border-related research and development. As modern border management involves technology and equipment that shows, to a large extent, an overlap with the needs of modern armed forces, there is a clear potential for synergies.
The first phases of developing Eurosur will be completed by the end of 2013. Although Eurosur is mainly about linking already existing surveillance assets of member states and other EU agencies, a lot of funds and efforts are devoted to research and development. Investments in satellite tracking systems, coastal radars, RPAS and autonomous targeting systems can clearly be beneficial to the wider security sector, including defence. Synergies with the defence sector for dual-use technologies and capacities should be fully exploited.

EU-wide situational pictures (including pre-frontier) and the exchange of information across sectors would be very valuable for armed forces and CSDP operations. The defence sector could be included in the user community, but this will require new Council decisions as currently border security networks and systems cannot be use by the military. In parallel synergies between the civil and military actors should also be fully exploited in the national context. Synergies are not limited to dual-use technologies: also CSDP could learn and benefit from what is achieved in border management. The 2011 Frontex regulation reflects the priority of border control. The strict provisions (including penalties) for member states once they have agreed to supply personnel and equipment for Frontex's European Border Guard Teams pool and Technical Equipment Pool may serve as an example of a best practice for EU defence, moving from voluntarism to a situation of obligations. The differences are clear: border management is an area of shared competence between the member states and the Commission, while defence is an exclusive member state compe-

93 Ibidem.

tence. Nevertheless, the experiences gathered with Frontex could find their way into a CSDP which is looking to increase its effectiveness.
Although the expertise of Frontex seems indispensable for dedicated border management CSDP operations, such as EUBAM Moldova and EUBAM Libya, there is also a potential for contradictory policy goals. On the other hand, the involvement of agencies as Frontex in CSDP operations can endanger the EU's comprehensive approach in crisis management. In the planning and conduct of CSDP missions this should be taken into account.

Another example of a best practice could be Article 7 of the 2011 Frontex regulation, which allows the agency to buy or lease equipment by itself or acquire it in co-ownership with member states. This article can be regarded as a model for how the EU could continue to own or lease dual-use assets to provide the whole EU security sector (including defence) with key enablers. The wish of the Commission to facilitate the security sector in the EU with assets that member states are unable to acquire themselves has been reaffirmed in the 2013 Commission Communication in preparation for the December European Council. It can be envisaged that Frontex's article 7 which provides a 'model agreement' for the co-ownership of assets by the EU and a member state (or a group of member states) can find broader application. The article, for example, makes arrangements about the availability of the assets.

The border management area is developing at a fast pace. Although complications regarding legal frameworks, stove-pipe policies, differing competences, modus operandi, sovereignty issues, ethical objections and political priorities make it difficult for the defence sector to hop onto this speeding train, the potential is clear. The two worlds are mutually reinforcing, but one of the first problems to overcome seems to be that they are still relative strangers.

4 Case study cyber security

Importance

"Cyberspace has become part of the daily life of many governments, citizens, industry etc. around the world. Moreover the global expansion of digital media, networks, and information and communications technologies (ICTs) might well become the most powerful technological revolution in the history of human kind", according to a United Nations publication.[94] However, the benefits of this revolution come with risks and costs. Civil society, the private sector, governments, and militaries are increasingly dependent on networked ICTs, which creates new vulnerabilities to personal, national, regional and global security. According to the EU High Representative, "There are an estimated 150,000 computer viruses in circulation daily, and a similar number of computers are compromised every day. The cost of cybercrime is hundreds of billions of euros every year. Cyber attacks on major international organizations and governments have become a daily reality".[95]

References to cyberspace sometimes suggest that it is a distinct 'space' that has no relationship to time, place or human action. However, cyberspace is nothing more or less than the sum of all ICT equipment, data and services.
Cyber security can be defined as "freedom from danger of damage due to the disruption, breakdown, or misuse of ICT. The danger or damage resulting from disruption, breakdown, or misuse may consist of limitations to the availability or reliability of ICT, breaches of the confidentiality of information stored on ICT media, or damage to the integrity of that information".[96]

EU Cyber Strategy

Many EU documents on cyber security have been published during the last few years.[97] The European Security Strategy update of 2008 included cyber threats

94 *The Cyber Index: International Security Trends and Realities*, United Nations Institute for Disarmament Research, Geneva, Switzerland, 2013, p. ix.
95 *Remarks by EU High Representative Catherine Ashton at press conference on the launch of the EU's Cyber Security Strategy*, Brussels, 7 February 2013.
96 *National Cyber Security Strategy: Strength through Cooperation*, Dutch Ministry of Security and Justice, The Hague, 22 February 2011.
97 *National Cyber Security Strategies, Practical Guide on Development and Execution*, European Network and Information Security Agency, December 2012, pp. 2-6.

as a new risk to European security.[98] The EU is active in two cyber security areas that overlap significantly: measures to combat cyber attacks including cybercrime, and measures to support critical infrastructure protection and network security. Relating to cyber issues, "the Common Foreign and Security Policy is underdeveloped – in part due to its confidential and interdepartmental nature, but also due to the difficulties in approaching the subject perceived to be a matter often left to Member States" according to a European Parliament Study.[99]

In February 2013 the EU Cyber Security Strategy was adopted.[100] This Strategy is accompanied by a legislative proposal (a Directive) from the European Commission to strengthen the security of information systems in the EU. This would encourage economic growth as people's confidence in buying goods online and using the internet would be strengthened. The Directive must pass through the Council of Ministers and the European Parliament before adoption, which is expected in 2014. The draft Directive sets out a number of proposals designed to enhance the EU's resilience to cyber security threats.[101] The Directive gives an indication of how regulation in this area may develop over the coming years. The Directive has two aims. The first is to ensure that member states and those private undertakings providing certain critical infrastructure within the EU have an adequate strategy, and take appropriate steps to deal with cyber security threats. The second aim is to facilitate information sharing about cyber security threats between the public and private sectors and between member states. The Directive also sets out in broad terms the obligations that member states will be expected to impose at industry level.

The Cyber Security Strategy does not foresee any legislation at this point. Nevertheless, it reflects the awareness that coordination across a range of policy areas in Europe is necessary to respond to the challenges of cyber security. The Strategy is remarkable in the way that it coordinates policy across three areas whose competences and mandates used to be separated: law enforcement (under Commissioner Cecilia Malström), the 'Digital Agenda' (under

98 *Report on Implementation of the European Security Strategy* (see footnote 4).

99 *Cyber security and Cyberpower: Concepts, Conditions and Capabilities for Cooperation for Action within the EU*, European Parliament, Director-General for External Policies, Policy Department, 2011.

100 *Cyber Security Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 7 February 2013.

101 Simon Shooter, Joseph Jackson and Toby Bond, 'Cyber security and the EU: regulating for network security', *Bird & Bird*, 1 July 2013.

Commissioner Neelie Kroes), and defence, security, and foreign policy (the High Representative for Foreign Affairs and Security Policy Catherine Ashton). The Strategy has three aims: (1) to strengthen the security and resilience of networks and information security systems, (2) to prevent and fight cybercrime, and (3) to establish a more coherent cyber security policy across Europe. The Strategy is a high-level document with such goals as improving the resilience and capacity of EU member states, strengthening the fight against cybercrime, addressing and developing structures and capabilities for EU cyber defence, and formulating an international policy on cyber security to help build capacity outside the EU.

An important aspect is the effort to harmonise the cyber security capabilities of EU member states. This has been defined as ensuring that EU countries properly equip themselves to tackle network and information security. In this field not much progress has been made. The Strategy will require that each EU member state possesses a well-functioning national-level *computer emergency response team* (CERT) and a competent authority to speak on behalf of the country in European-level discussions. This is easier said than done, as member states have varying types of responding authority, and not all can formulate a national-level response. The question arises whether promoting incident response teams – organisations with a reactive mind-set – will influence how a country tackles these issues at a national level, undermining a more proactive approach. An analysis of the culture and practice of CERTs suggests that where they lack a strong legal basis, CERTs regularly find themselves operating in the dark with respect to what data they can and cannot share across borders or even with other organisations within their own country (such as law enforcement). However, CERTs do communicate, exchange information and share malware signatures informally, i.e. via FIRST, a community of CERTs.

Following a feasibility study conducted by Rand Corporation Europe, the European Commission decided to establish a European Cybercrime Centre at Europol, which was opened in The Hague on 11 January 2013.[102] The Centre will be the focal point in the EU's fight against cybercrime, contributing to faster reactions in the event of online crimes. It will support member states and the European Union's institutions in building operational and analytical capacity for investigations and cooperation with international partners. The Centre will provide support to enhance national capabilities to investigate and combat cybercrime, and encourage the implementation of cybercrime directives.

102 See www.europol.europa.eu.

The Cyber Security Strategy also aims to strengthen cooperation between the public and private actors, to encourage the development of public-private partnerships, and to take advantage of other initiatives, such as the European Public-Private Partnership for Resilience (EP3R). However, it faces challenges over its direction and participation, and it lacks a sufficient robust and diverse group of stakeholders (especially end-users of technology). EP3R is attempting this year to re-energise its activity under the facilitation of the European Network and Information Security Agency (ENISA). It is not clear to what extent industry has been motivated to engage in EP3R by the perception that it is a suitable channel to influence policymakers in Brussels.

Civil-military aspects

An important aspect of a more coherent EU cyber security policy is the development of capabilities, encouraging dialogue and cooperation between the military and civilian sectors. The EU Cyber Security Strategy brings the contributions of defence and foreign policy to cyber security under one framework, but a great deal of work has to be done before cyber security is integrated into the European Common Foreign and Security Policy (CFSP). It is a point argued for by High Representative Catherine Ashton.

One of the major problems with the civil-military dimension of the EU Cyber Security Strategy is the clash between the need for concepts, structures and doctrine at the EU level, while security and defence continue to be bastions of national sovereignty. Under the European Union Military Staff, the EU only has a nascent cyber defence concept for its own networks. To support this, RAND Europe has provided the EDA with a benchmark assessment of the levels of military cyber defence capability across the EU. In May 2013 the EDA presented the results of the study, The RAND study identified opportunities both for the national and the international level. At the national level, greater attention should be given to the development of cyber defence training and education initiatives. The study encourages participating member states to consider exchanging information on equipment solutions and pooling & sharing for cyber defence capabilities, and on processes and shared escalation procedures, especially EU-led missions. The study also suggests that participating member states should consider sharing – to a certain extent – facilities and to take into account interoperability aspects of cyber defence. At the European level, the study emphasises that military cyber defence is in general at a relatively early stage of maturity. The study makes high-level recommendations such as enhancing EU network protection, strengthening intelligence capability, deepening incident response capabilities, creating a culture of cyber security, promulgating security

standards and tools, and reinforcing links between NATO and the EU for cyber defence issues. To avoid duplication, the EU will explore possibilities of how the EU and NATO can complement their efforts to heighten the resilience of critical governmental, defence and other information structures on which the members of both organisations depend.

The EU is also promoting the early involvement of industry and academia in developing solutions and in strengthening Europe's defence industrial base and associated R&D innovations in both civilian and military organisations. The EDA will promote civil-military dialogue and contribute to the coordination between all actors at EU level – with particular emphasis on the exchange of good practices, information exchange and early warning, incident response, risk assessment and establishing a cyber-security culture.

In her final report for the December 2013 European Council the High Representative has repeated her call for seeking synergies between the civilian and military actors in Europe in responding to cyber threats. She has called for a Cyber Defence Policy Framework, focusing on capability development, training education and exercises. The Policy Framework should define the division of tasks between the member states and CSDP structures in areas like capability development, protection of networks supporting CSDP, training and education opportunities, cooperation with NATO, developing early warning and response mechanisms.[103]

Given that threats are multifaceted, synergies between civilian and military approaches in protecting critical cyber assets should be further enhanced. European military and civil cyber-security stakeholders will have to work much closer together to boost Europe's network and information security (ENIS) in the future. The EU has in principle the regulatory instruments to implement a civil-military approach. But the role of the military in defending against cyber risks has yet to be fully defined and understood.[104]

103 *Final Report by the High Representative* (see footnote 21).

104 Neil Robinson, Agnieszka Walczak, Sophie-Charlotte Brune, Alin Esterle, Pablo Rodriguez, *Stocktaking study of military cyber defence capabilities in the European Union (milCyberCAP)*, Unclassified Summary, RAND Europe, 2013.

National approaches[105]

Nowadays, the majority of EU member states have some kind of national effort and approach to secure critical networks and to respond to cyber threats. National cyber security efforts can be roughly divided into two general categories: those involving only domestic agencies (usually communications ministries or law enforcement agencies) and those where the national military also have a cyber security role. In the following, one example of the first category (the Czech Republic) and two examples of the second category (Germany and the Netherlands) will be addressed.

Czech Republic

The Cyber Security Strategy of the Czech Republic for 2011-2015 provides the basics for future Czech security policies and legal standards.[106] The underlying objective of this Strategy is to protect ICT infrastructure from cyber threats and to mitigate the consequences of attacks if they occur. The Czech Republic released Decision 781 in October 2011, establishing the National Security Authority, charged with cyber security. This decision also established the National Centre for Cybernetic Security (NCCS), which coordinates with Czech and international CERTs and undertakes research and development.[107]
The Strategy considers cyber security to be the responsibility of the government, the private sector, and the general population. As a result the government will draft legislation to determine the responsibilities of the relevant public authorities for establishing cyber security standards for the government, the private sector, and individual computer users. The Czech Republic plans to enact legislation to establish security standards for critical infrastructure, and to create a national CERT that will provide cyber threat early warning and optimise response capabilities.

The Czech Republic will become involved in international cooperation in the field of cyber and information security. Within the EU and the NATO, it will participate in the drafting of standards and international policies, as well as in

105 This section is mainly based on Hans Bouwmeester, Hans Folmer & Paul Ducheine, 'Cyber Security and Policy Responses', in: Paul Ducheine, Frans Osinga, Joseph Soeters (eds.), *Cyber Warfare: Critical Perspectives*, T.M.C. Asser Press, The Hague, pp. 19-49; *National Cyber Security Strategies, Practical Guide on Development and Execution*, European Network and Information Security Agency, December 2012, and *The Cyber Index – International Security Trends and Realities*, United Nations Institute for Disarmament Research, Geneva, 2013.

106 *Cyber Security Strategy of the Czech Republic, for the 2011-2015 Period*. See: www.cybersecurity.cz.

107 *What is NCK*, Czech National Cyber Security Center. See: www.govcert.cz.

activities of joint institutions, and, at the same time, adequately apply the standards and relevant mechanisms in its own national cyber security legislation.

The Ministry of the Interior coordinates cyber security issues.[108] The National Security Research Strategy (NSRS), approved in 2008, includes the protection of critical infrastructure, and is implemented by the Ministry of the Interior, which has a Cyber and Informational Security Department.[109] The Czech Armed Forces established a Computer Incident Response Capability (CIRC) in January 2007.[110] As a part of this centre the Computer Emergency Readiness Team (CERT) was founded. CIRC helps commanders and management in the decision-making process, but also to achieve and maintain a secure and reliable information and communications environment in several areas like operational safety and the active cyber defence of communication and information systems. CIRC plays an important role in the Czech Army overall and especially in computer network security. However, it is mainly focused on security monitoring, rather than routine traffic monitoring.

Germany

The German Federal Government released a new cyber security strategy in March 2011.[111] This strategy focuses on ten strategic areas, which can be grouped in the following clusters: (1) the protection and security of German critical networks and systems, (2) the setting up of a National Cyber Response Centre (NCRC) and a National Cyber Security Council (NCSC), (3) effective cybercrime control, (4) international cooperation, and (5) personnel development in federal authorities. The NCSC is headed by a state secretary from the Ministry of the Interior. The Ministry of the Interior leads on cyber security. The Federal Office for Information Security, overseen by the ministry, is in charge of promoting the security of information technology.[112]

The NCSC focuses on coordinating preventive and cooperative cyber security measures. It is composed of the Federal Chancellery and state secretaries from the Foreign Office, the Ministry of the Interior, the Ministry of Defence, the Ministry for Economics and Technology, the Ministry of Justice, the Ministry of Finance, and the Ministry of Education and Research, as well as state representatives. Representatives from private industry as well as academia are invited as

108 *Cyber Security in the Czech Republic.* See: www.cybersecurity.cz.
109 *Czech Republic Country Report*, European Network and Information Security Agency, 2011, pp. 5 and 13.
110 See, Josef Kaderka, Milan Jirsa, *Cyber Defence in the Armed Forces of the Czech Republic*, http://ftp.rta.nato.int
111 *Cyber Security Strategy for Germany*, German Federal Ministry of the Interior, 2011, pp. 9-10.
112 Ibidem.

associated members. The NCSC is responsible for coordinating defence techniques and cyber policy.[113]

The NCRC incorporates officials from the Federal Criminal Police Office, the Federal Police, the Customs Criminological Office, the Federal Intelligence Service, the Armed Forces, and Critical Infrastructure authorities. The Centre reports to the Federal Office for Information Security and coordinates with the Federal Office for the Protection of the Constitution and the Federal Office of Civil Protection and Disaster Assistance (both parts of the Ministry of the Interior).[114] The Centre will not develop offensive capabilities, but focuses on international cooperation and information sharing in areas of vulnerability protection and incident response. In August 2012 the Minister of the Interior announced the potential need for new cyber security legislation and that he was currently in discussions with industry.

Civilian cyber security focuses on all ICT systems for civilian use in German cyberspace, while military cyber security focuses on all ICT systems for military use in German cyberspace. The Department of Information and Computer Network Operations of the Armed Forces' Strategic Reconnaissance Unit is tasked with developing cyber capabilities. It is testing the latest methods of infiltrating, exploring, manipulating, and destroying networks. The unit, known by its innocent official name 'Department of Information and Computer Network Operations', is preparing for an electronic emergency, including digital attacks on outside servers and networks.[115]

The Netherlands

The Netherlands issued the National Cyber Security Strategy (NCSS) in February 2011.[116] A new version will be published in November 2013, only two years after the first. The reason for this is the changing cyber landscape and the fact that most of the goals have been realised. The Strategy has five components: (1) linking and reinforcing initiatives, (2) promoting individual responsibility, (3) creating public-private partnerships, (4) pursing international cooperation, and (5) striking a balance between self-regulation and legislation. It calls for annual trend reports in cybercrime and digital security. The Strategy places strict emphasis on regulating cybercrime and it launched an initiative to ensure that all information and communications technology parties report data

113 Ibidem.
114 Ibidem., p. 8.
115 J. Goetz, M. Rosenbach and A. Szandar, 'National Defense in Cyberspace', *Der Spiegel Online International*, 11 February 2009. See: www.spiegel.de.
116 *The National Cyber Security Strategy: Strength through Cooperation* (see footnote 96).

loss, theft, or misuse. There will also be a Cyber Education and Training Centre to research cyber defence and to develop human capital to bolster a growing digital economy. As a result of the NCSS the National Cyber Security Council (an independent advisory body for the Dutch Government) was established on 30 June 2011.

The National Cyber Security Centre was created on 1 January 2012 with the purpose of providing expertise and advice, and monitoring threats and managing crises, and encompasses the previously existing GOVCERT NL. The Centre has published a security checklist for supervisory control and data acquisition for industrial control systems, and the Cyber Security Assessment Netherlands report, which assesses the short-term goals and needs of the government regarding cyber security.[117] The National Coordinator for Counter-Terrorism has expanded its mission to include a cyber component, specifically in testing the vulnerability of internet applications against cyber attack.[118]
The Ministry of the Interior coordinates interdepartmental cyber security among various civilian and military units responsible for cyber issues. The Ministry of Defence plans to invest in the development of cyber warfare capabilities despite budget cuts in other areas. The Netherlands has a memorandum of understanding with Luxembourg and Belgium on cooperation in cyber security, including information sharing and expertise sharing, cooperation on best practices, and the development of public-private partnerships.[119]

The Dutch Ministry of Defence released its Defence Cyber Strategy (DCS) in 2012.[120] The Strategy addresses six specific priorities: a comprehensive approach, enhancing defensive capabilities, developing offensive military capabilities, improving information gathering and security skills, improving and encouraging innovation, and continuing to foster and develop domestic and international cooperation efforts. The Strategy describes the offensive capabilities as a "force multiplier" for increasing military effectiveness and preserving an "active defence", while recognizing the reality that the use of cyber techniques as a military tool is still in its infancy.

The military established the Cyber Taskforce in January 2012 in order to coordinate the reinforcement of the various cyber capabilities.[121] The cur-

117 *Cyber Security Assessment Netherlands*, Dutch National Cyber Security Centre, 2011; *Checklist Security of ICS/SCADA Systems*, 2012.
118 *The National Cyber Security Strategy* (see footnote 116), p. 12.
119 *Benelux sign memorandum of understanding on cyber security*, European Urban Knowledge Network, 12 April 2011.
120 *Defense Cyber Strategy*, Dutch Ministry of Defence, The Hague, 27 June 2012.
121 *Annual Report MIVD 2011*, 2012, pp. 49-50, 57.

rent activities of the armed forces include the establishment of a Defence Cyber Command (DCC) and a Defence Cyber Expertise Centre (DCEC). The armed forces are also in the process of developing a Defence Cyber Doctrine. Furthermore, a Joint Sigint Cyber Unit will be activated in early 2014 combining the intelligence efforts on cyber activities and threats as well as creating closer coordination between the civilian and military intelligence services.
The Dutch Armed Forces have no responsibility in securing the networks of other public or private industry or agencies, nor is it their responsibility to combat cybercrime. However, in case of an emergency and upon request the Netherlands Ministry of Defence can under the policy of 'Intensifying Civil-Military Cooperation' contribute with its cyber capacity to support the civil authorities. On the other hand, civil cyber capacities can also support Defence in emergency situations. In other words, internal and external security in the field of Dutch cyber security are intertwined.

The way forward

Coordination, collaboration, dialogue and information sharing are the buzzwords within the EU in the field of cyber security. But cyber security is still mainly a 'free for all' business. EU member states still have a different level of awareness regarding cyber threats. Also in terms of countering those threats: some member states are quite advanced in their technological competence as well as internal structures, while others are much less so, as different studies have highlighted.
The European Union should play an important role in setting and discussing norms and debating resilience measures to support member states. However, in terms of technical, legal and political harmonised measures, there are still significant differences between individual member states and EU institutions.

Although the European Cyber Security Strategy has received a great deal of attention because of its comprehensive character, two significant issues are important. First, institutional turf wars should be ended in order for the Strategy to become a practical reality. As is well known, inter-institutional battles between different directorates can be discouraging. Second, the Strategy will undoubtedly need an accompanying action plan to detail how it will work in practice. This is particularly the case in the current climate of austerity. The action plan should also contain guidance for evaluation to identify and robustly measure the effect of the Strategy. Otherwise, the high-sounding remarks about cooperation might start to sound very hollow indeed. However, the Commission proposal of 7 February 2013 for a Directive should be a leading imperative.

Different studies have made clear that EU member states need to have flexible and dynamic cyber security strategies. It is obvious that the cross-border nature of threats makes it essential to focus on strong international cooperation. This has been recognised by most national cyber security strategies. Cooperation at the pan-European level is necessary to effectively prepare for, but also to respond to cyber-attacks. ENISA considers comprehensive national security strategies as the first step in this direction.[122] And the RAND Europe study emphasises that military cyber defence on the European level is still at a relatively early stage of maturity. But most important is the political will which is required to implement all the recommendations which are made in these studies. The national implementation of EU-binding rules which will be included in the Commission's proposed Directive is necessary to make cyber security a practical reality in the EU in the near future.

122 *National Cyber Security Strategies* (see footnote 97), pp. 1-2.

5 Conclusions and recommendations

Conclusions

Europe's security is no longer the sole realm of foreign policy and defence. The days of separating external and internal security are over. The traditional 3D tools – diplomacy, defence and development – are still hardly needed to deal with crises outside Europe, but many other sectors of government have to be involved to cope with their effects at home. External security has become internal security and vice versa. European citizens see their security less threatened by armed conflict than by the consequences of illegal immigration, international crime, terrorism, the interruption of trade and energy flows, disasters and drugs trafficking.

Security has become wider than during the Cold War and its immediate aftermath. Today and tomorrow European security will be determined by a broad mix of threats and challenges, which will require different responses than in the past. External and internal security instruments will have to be increasingly connected, if the European Union and its member states want to deal effectively with those threats and challenges. It implies that both actors and means have to come together. Foreign Affairs and Defence have to be connected to Justice and Home Affairs, Transport and other government sectors in order to generate integrated responses. In the same manner it will be necessary to combine civil and military assets to create optimal capacities to strengthen European security. The European Union is in need of an integrated approach to security.

The need to connect external and internal security is widely acknowledged, both in the European Security Strategy – driven by the external actors – and in the EU's strategies and policies dealing with internal security, maritime security and cyber security. Yet, an integrated approach does not exist and the capacities remain separated. At best the military are requested to assist on an ad hoc basis, such as deploying reconnaissance aircraft, ships and military personnel to operations of the external border agency Frontex. Also, the exchange of maritime surveillance data between the European Maritime Safety Agency and the command of the EU anti-piracy Operation Atalanta near the Horn of Africa has been arranged on an ad-hoc basis. No structural coordination and operational

connections exist between the EU's actors in the external and internal security realms. The reason for this is clear: the legal distinction under the EU Treaties between the intergovernmental Common Foreign and Security Policy (CFSP), including the Common Security and Defence Policy (CSDP), and the predominantly communitarian areas like Justice and Home Affairs or maritime transport creates barriers which are difficult to overcome. It has an impact on many aspects, from decision-making to organisation and from finance to parliamentary control.

Unfortunately, the legal dimension is not the sole provider of obstacles to integrated security. Vested interests, organisational culture and bureaucratic turf battles are equally responsible for continuing business as usual. This is not a specific phenomenon related to the Brussels level. As the case studies show, capitals face the same problem of stove-piped organisations and a lack of willingness to coordinate or integrate. In particular the Justice and Home Affairs Ministries traditionally fear a 'militarisation' of internal security. National security strategies with whole-of-government theory are no guarantee for a well-implemented whole-of-government approach in reality. It also seems that practical solutions are easier to realise in smaller countries (the Netherlands) than in bigger nations (Germany, the United Kingdom). This might be the logical consequence of larger numbers of actors involved and more complicated organisational structures in larger nations. But history and geography also play their role. For example, the differences in the national approaches to maritime security can to a certain extent be explained by a continental orientation (Germany) or by a seaborne tradition (the Netherlands, the UK). The upshot is that overcoming the gap between external and internal security is not just a matter of slashing legal barriers, which in itself is already complex and hard to realise. Another conclusion is that closing the gap requires change both at the EU and the national level. An integrated European security strategy will not work when at the national level separated worlds continue to exist.

The Lisbon Treaty has not ended the legal separation of intergovernmental and communitarian responsibilities, but it offers potential for bridging the gap. The Solidarity Clause for mutual assistance in case of terrorist attacks or disasters opens the possibility of deploying civilian and military assets together. Article 185 offers scope for Union funding of defence research and technology programmes of member states. The 'translation' of these two articles into policy has shown that political, legal and bureaucratic opposition is hard to overcome. The implementing policy of the Solidarity Clause – as proposed by the relevant EU authorities, but no doubt after political consultations with member states – is much weaker than the potential offered by the Treaty text. The legal and

bureaucratic resistance in some parts of the European Commission succeeded until recently to block the use of article 185. The Commission's Communication of late July 2013 incorporated a positive interpretation, which can be seen as a late but nevertheless important breakthrough.
The two examples underline how slow and complex the decision-making machinery operates when it comes to formal steps based on Treaty articles. However, in certain areas this will be needed, in particular when it comes to formal relationships between intergovernmental CSDP actors and those operating in the communitarian field. A structural exchange of information between the military and EU civilian security bodies and agencies will only become possible if at Council level new decisions are taken to enable such a data flow. As sector-related Council formations are unlikely to take such decisions, the European Council should steer and direct the process of developing the necessary legal arrangements to allow for civil-military interaction between external and internal security players.

In the meantime practical measures can further enhance the connectivity between both sides. For operations the EU and member states can build on the positive experiences with maritime surveillance data exchange, military support to Frontex, advice by internal security actors to CSDP missions and other examples. For capability development the European Defence Agency has shown the way by connecting military requirements to civilian user needs for dual-use capacities in areas like communications, reconnaissance, intelligence and air transport. The Commission's Communication for the December 2013 European Council offers more scope, not only for dual-use technology research but also for the use of capacities, both by civilian actors and the military, financed by the Union budget. This Commission proposal will make it possible to acquire and operate EU transport aircraft, remotely piloted aircraft systems, deployable medical facilities or CBRN defence equipment either for civilian or military use. The European Council should wholeheartedly welcome the proposal and ask the Commission to implement it as soon as possible.

Recommendations

General

1. As external and internal security can no longer be separated the European Union needs an *integrated security approach* which frames all existing strategies and policies.
2. The integrated security approach needs to be developed *at the EU level and at the national level* in parallel in order to create consistency and effectiveness between EU and member states' actions.

3. The British example of *parliamentary scrutiny* of the implementation of the national security strategy *by a Joint Committee* is also needed in other EU member states and in the European Parliament to overcome stove-piped approaches in those parliaments.
4. The European Council should define objectives and issue guidance for *slashing legal barriers* which block the *structural coordination and integration of civil and military capacities*, such as for data exchange and for arrangements in order to make use of each other's assets.
5. The potential of the *Solidarity Clause* (Art. 222 TFEU) should be fully exploited in implementing arrangements, including for *military support to civil authorities.*
6. The scope for seeking *synergies on dual-use research* under the Horizon 2020 programme with defence R&T should be *systematically checked and fully exploited* between the European Commission, the European Defence Agency, member states and other organisations like the European Space Agency.
7. The European Commission's proposal on *co-funding defence research projects* on dual-use technologies of member states should be *implemented quickly* through a Preparatory Action. Collaborative R&T projects in EDA should be the first candidates for such co-funding.
8. The scope for *EU-owned dual-use capacities in areas like remotely piloted aircraft systems* (RPAS) should be *explored as soon as possible*, not only in coordination with the European External Action Service but also with member states.

Maritime security

9. The EU maritime security strategy has to be *global*, *civil-military* and *comprehensive* with its *governance* based on the *legal responsibilities* of the actors involved and with an *integrated structure* to the extent possible in terms of operational instruments, civil and military.
10. EU maritime security *capabilities* will require *planning coordination* between all ministries involved and at the EU level between the CSDP, maritime policy and internal security actors, including the relevant EU agencies.
11. Under the *Common Information Sharing Environment (CISE)* initiative priority should be given to prepare for Council decisions on the required *legal arrangements* to allow for *structural maritime surveillance data exchange* between all relevant civil and military, national and EU level actors.
12. In order to speed up the work on access rights and legal aspects *all relevant actors* should *meet together* regularly rather than only in their own sector environment.

13. The *integration of existing systems* into a *network of networks for maritime surveillance* is urgently needed. The experiences and lessons learned from pilot projects, regional programmes and test beds for civil-military data exchange should be taken on board.
14. The *European Maritime Safety Agency* in Lisbon is the natural candidate to provide the central hub for *civil-military data collection and distribution*. EMSA should be *mandated* to develop this capacity.
15. *Civil and military maritime patrol aircraft* and other assets for maritime surveillance should be *pooled and shared* by coastal countries, to start with in regional clusters (Baltic Sea, North Sea, Atlantic approaches, Mediterranean).
16. *Civil and military search & rescue* capacities should be *combined at regional cluster level*.
17. *Training of civil and military personnel* involved in maritime security activities should be *combined* when possible in order to create commonalities and shared cultures. *Common exercises* should be organised, to start with at the level of regional clusters.

Border security

18. Border security is quickly expanding in the European Union, with the Frontex agency having a central operational role. As both civil and military capacities are needed for border security, *a structural approach to civil-military interaction* is urgently needed.
19. Modern border management involves *technology and equipment* that shows, to a large extent, an overlap with the needs of modern armed forces. There is clear potential for *synergies*, which needs to be fully explored.
20. Defence ministries in EU member states should incorporate the *availability of naval and other military assets* for Frontex operations in their *planning*.
21. For the *acquisition of own assets* Frontex should take into account *standardisation and interoperability* with the military and civilian capacities of *member states*.
22. The *Eurosur* data exchange network is a major step forward in support of border security in the EU. Other actors, including the *member states' armed forces*, should be *connected* to Eurosur for *a two-way street exchange of information.*
23. *Frontex support to CSDP operations and missions* with border control aspects should be carefully tailored to the objectives of those EU activities – in particular building functioning state institutions – and *not to install pre-frontier border checks*.
24. Frontex arrangements on the co-ownership of equipment with member states can be *applied* to relevant *dual-use assets purchased, owned and operated under the Union budget* as proposed in the Commission's Communication for the December 2013 European Council.

Cyber security

25. Cyber still being an area of large differences among member states, the *EU* should play an important role in setting and *discussing norms and debating resilience measures* to support them, both their *civil and military authorities*.
26. The EU Cyber Security Strategy will only work if *turf battles* between various Commission actors come to an end and the *action plan* and the *Directive* are agreed upon and implemented.
27. *Civilian and military approaches* in protecting critical cyber assets should be enhanced. European military and civil cyber-security stakeholders will have to work *much closer together* to boost Europe's network and information security (ENIS) in the future.
28. Member states need to have *flexible national cyber strategies*, which allow for the necessary *linkage* of their national cyber security assets and mechanisms *to EU-level cyber arrangements*.
29. As military cyber security measures show a mixed and generally immature picture, the recommendations of the *EDA study (*by RAND) should be *implemented*. Member states need to seek advice and assistance across a range of domains of military capability, such as doctrine, organisation, training, and interoperability.
30. National Cyber Emergency Response Teams (CERTs) should receive EU-level guidance on what *data* they can and cannot *share* across borders.

List of acronyms

AFSJ	Area of Freedom, Security and Justice
AIS	Automatic Identification System
BlueMassMed	Blue Maritime Surveillance System Mediterranean
CBRN	Chemical, Biological, Radiological and Nuclear
CERT	Computer Emergency Response Team
CFSP	Common Foreign and Security Policy
CIRC	Computer Incident Response Capability
CISE	Common Information Sharing Environment
COSI	Standing Committee on Operational Cooperation on Internal Security
CPIP	Common Pre-frontier Intelligence Picture
CRATE	Central Record of Available Technical Equipment
CSDP	Common Security and Defence Policy
DCC	Defence Cyber Command
DCEC	Defence Cyber Expertise Centre
DCS	Defence Cyber Strategy
DfT	Department for Transport
EBGT	European Border Guard Teams
EDA	European Defence Agency
EEAS	European External Action Service
EFC	European Framework Cooperation
EMSA	European Maritime Safety Agency
ENIS	Europe's network and information security
ENISA	European Network and Information Security Agency
EP3R	European Public-Private Partnership for Resilience
ESDP	European Security and Defence Policy
ESS	European Security Strategy
EU	European Union
EUBAM	European Union Border Assistance Mission
EULEX	European Union Rule of Law Mission
EUMS	European Union Military Staff
Eurosur	European External Borders Surveillance System

FIRST	Forum of Incident Response and Security Teams
FP7	7th Framework Programme
Frontex	European Agency for the Management of Operational Cooperation at the External Borders
GMES	Global Monitoring for Environment and Security
GOVCERT NL	Cyber Security and Incident Response Team of the Government of the Netherlands
GPS	Global Positioning System
ICMS	Intensifying Civil-Military Cooperation
ICT	Information and Communications Technologies
IMDATE	Integrated Maritime Data Environment
IMO	International Maritime Organisation
IMP	Integrated Maritime Policy
IT	Information Technologies
JHA	Justice and Home Affairs
KMar	The Royal Netherlands Marechaussee
LRIT	Long Range Identification and Tracking
MARSUNO	Maritime Surveillance North
Marsur	Maritime Surveillance
MCA	Maritime and Coastguard Agency
MERAC	Maritime Emergency Reporting and Assessment Centre
MFF	Multi-annual Financial Framework
MSSC	Maritime Safety and Security Centre
MSSIS	Maritime Safety and Security Information System
NATO	North Atlantic Treaty Organisation
NCC	National Coordination Centre
NCCS	National Centre for Cybernetic Security
NCRC	National Cyber Response Centre
NCSC	National Cyber Security Council
NCSS	National Cyber Security Strategy
NMIC	National Maritime Information Centre
NSRS	National Security Research Strategy
NSS	National Security Strategy
PSC	Political and Security Committee
RABIT	Rapid Border Intervention Team
RNL	Royal Netherlands
RPAS	Remotely Piloted Aircraft Systems

R&D	Research and Development
SDSR	Strategic Defence and Security Review
SGO	Seconded Guest Officer
SIGAT	Spectrum requirement for military UAS Insertion in General Air Traffic
SUCBAS	Sea Surveillance Co-operation Baltic Sea
TFEU	Treaty on the Functioning of the European Union
TEP	Technical Equipment Pool
TEU	Treaty European Union
UAS	Unmanned Aircraft Systems
UAV	Unmanned Aerial Vehicles
UK	United Kingdom
UKBA	United Kingdom Border Agency
VRMTC	Virtual Regional Maritime Traffic-Center
ZUIS	Zeevaart Uitbreidbaar Informatie Systeem

Civil-Military Capacities for European Security

Contrary to the past external and internal security are now interwoven. Instability and conflicts outside Europe affect the security in European countries through terrorism, illegal immigration and international crime. Cyber attacks can come from any corner in the world. The security of the seas is threatened by a wide variety of dangers, most of whom are of a non-military nature. Internal security has become external security and vice versa.
The European Union and its member states have to adapt their strategies and policies to this new environment. Security needs an integrated approach, encompassing all relevant sectors of government. Equally, civil and military capabilities can no longer be treated separately. The scope for a more coordinated and integrated way of developing and using civil-military capacities should be fully explored.
This Clingendael report argues for closing the external-internal security gap. The authors address three specific cases: maritime security, border security and cyber security. The report provides thirty recommendations for the development and use of civilian and military capabilities for European security in a more coherent and structured way.

About the authors

Margriet Drent, Kees Homan and Dick Zandee are Senior Research Fellows at the Clingendael Institute.

The Netherlands Institute of International Relations 'Clingendael' is an Independent institute for research, training and public information on International affairs. It publishes the results of its own research projects and the monthly Internationale Spectator and offers a broad range of courses and conferences covering a wide variety of international issues.

Clingendael
Netherlands Institute of International Relations