WP4
Political leadership, European institutions and Transboundary Crisis Management Capacity

Deliverable D4.1
Inventory of Commission, European Council & Council of the European Union Crisis Capacities

Authors: Mark Rhinard & Sarah Backman, Stockholm University

Delivery date: 30 March 2017

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 649484

Table of Contents

Contents

Executive Summary

Introduction

This report inventories the crisis management capacities of the European Commission, Council of Ministers of the European Union, and the European Council. It responds to a central concern in the Transcrisis project: that the 'institutional capacities in the three institutions need to be better measured in terms of how they contribute to preparation, response, and recovery' (Transcrisis proposal, p. 34). Capacities are defined in terms of politico-administrative features that facilitate the pursuit of seven tasks of effective crisis management, defined by the project as: *detection, sense-making, decision-making, coordination, meaning-making, communication and accountability*. Investigating capacities in seven issue areas, we reveal a host of emerging capacities in recent years (roughly 200 in total). Some of these capacities were expected, others are surprising. When compared with previous studies, the results show intriguing trends in how, where and in what forms capacities have evolved in recent years. While this report serves as a stand-alone deliverable with its own essential findings, it also provides the foundation for further exploration of effectiveness, legitimacy and leadership across Transcrisis sub-projects.

Methodology

Data collection for this project began on 1 October 2015 and ended on 30 March 2017. The research team applied the analytical framework inspired by the Transcrisis 'codebook'. The codebook lists seven key tasks – stated above – which expand on the traditional cycle of prevention, preparation, response, and recovery (with an emphasis on preparation and response). We combined sense-making/communication into a single category because it was difficult to find mutually exclusive capacities for either one.

We applied the remaining analytical categories to seven major issues areas:

- Transport, health, cyber, energy, terrorism, civil protection, and migration.

Primary sources used include the EU institutions' websites in addition to the EU's legislative and pre-legislative databases. Official documents and web-site presentations provide the bulk of the data presented here. Some participant interviews were conducted, but on a largely unsystematic basis and will in the future be systematised. *Secondary sources* include think-tank and academic articles on the topic. Sectoral-focused studies were used to quality-check our primary sources when possible (few scholars study EU crisis management in a cross-sectoral and cross-national way, however). When faced with doubts on the relevance of certain capacities, we erred on the side of inclusion rather than exclusion. This report is largely deductive in methodology, using an existing framework to collect data, but allows for a degree of inductive theorising.

Within each issue area, internet research proceeded in three steps. It started by examining Commission issue-specific websites (largely found in individual Directorates-General websites). It was complemented by in-site Google searches for Transcrisis-project lexicon like 'crises', threats', 'emergencies', 'disasters', 'preparedness', 'early warning', and 'urgent'. Then, researchers turned to EU legislative databases such as Eur-Lex. Finally, secondary sources – analytical studies – were consulted to see if any data escaped our earlier searches. Some capacities are placed in multiple categories, when they serve multiple crisis management tasks (thus, the number 165 above is a rough approximation). Units, platforms or centres with multiple capacities are listed in each respective category. All sources are dated and documented in the attached volume. Please note that further research is needed to complete the capacity inventory for the Council of Ministers and European Council.

Looking across the issue areas, we now turn to common findings in each analytical category.

Findings

Detection

We operationalised detection by searching for EU capacities relevant to 'the timely recognition of an emerging threat' (Transcrisis codebook, p. 11). In practice, this involved searching for EU activities on threat monitoring, horizon scanning, and early warning.

We found an abundance of EU capacities here. Roughly speaking, the capacities number 45. Few EU policy areas lack monitoring or early warning tools. From transport disruptions to air quality problems, detection efforts are present. Moreover, few conceivable threats are without a specific detection system. By way of example, the health field has five detection systems for five different types of disease. CBRN threats from an intentional source are treated in a system (RAS-BICHAT) that is separate from CBRN threats from accidental sources (RAS-CHEM). Each transport sector – air, sea, and rail – has systems in place at the European level to detect emerging threats. Detection of third country nationals crossing EU borders takes place (albeit with some difficulties as seen in the current migration crisis) in three systems: EURODAC, the Visa Information System (VIS) and the recently proposed Entry-Exit System (part of the Smart Borders package of proposals).

Unsurprisingly, perhaps, systems are particularly pronounced in areas that experienced recent attacks or emergencies. Warning systems for energy crises – namely gas and oil – have been put in place. Following the Icelandic Ash Cloud, Eurocontrol's Pilot In-Flight Reports system collects real-time information about ash cloud positions and concentrations. Potential cyber- and terrorist-attacks – the detection focus *de jour* -- are now monitored by no less than two systems each, started in 2015.

Perhaps as a result of proliferation, we also note consolidation efforts. 'Systems of systems' seem to be on the rise when compared to previous research (Boin et al. 2006; Boin et al. 2014). COPERNICUS provides a ‘rapid mapping’ facility to spot potential environmental problems from earth and space, drawing together existing systems like the EFAS (flood alert) and the EFFIS (forest fire warnings). DG Santé’s Epidemic Intelligence Information System (EIIS) draws in various health systems under a common platform. And ARGUS, although dating back to 2006, is undergoing revision. ARGUS is the Commission Secretariat-General’s effort to build a single platform for all detection systems. At least one Commission insider told of us a cat-and-mouse game: real crises lead to new detection systems, which in turn lead to efforts to link them together after initial attention fades. We revisit this hypothesis in the last section below.

Sense-making

Sense-making refers to ‘the collection, analysis, and sharing of critical information that helps to generate a shared picture of an impending crisis’ (Transcrisis codebook, p. 11). In practice, this meant searching for EU tools related to: situational awareness, common situation pictures, risk assessment, analysis of information from detection or distribution of information, information-sharing practices for creating a common situational picture or to create a basis for decision making.

Our results were surprisingly robust here, especially when viewed in temporal perspective. In recent years, much work has gone into the Council’s Integrated Situation Assessment and Analysis (ISAA) function, for instance, which allows the Secretariat-General of the Council to provide a situation assessment in the outbreak of a crisis. In civil protection, many resources have been directed towards understanding the breadth and impact of an emerging disaster, via technological tools housed in the ERCC. Our nomenclature of ‘sense-making’ is even used by officials to describe their efforts. In critical infrastructure protection, the CIWIN system (critical infrastructure warning and information network) not only collects information about problems in different infrastructures but also ‘enriches’ the data through analysis. A new unit to spot terrorist financing has been placed in Europol, built around an ‘FIU.net’ network of information sharing and situation assessment. Following the 2010 Ash Cloud crisis, Eurocontrol’s EACCC (European Aviation Crisis Coordination Cell) seeks to get ‘ahead of the game’ when major aviation failures occur by providing early analysis Europe-wide. European Border Guard Teams engage in a form of sense-making when they assess ‘pressure points’ and report to central authorities. One last example (see the attached inventories for more) can be found in the field of cyber-security, where the newly established CSIRT network shares information and discusses problems amongst national experts.

Sense-making tools herein fall into two broad categories. The first is sense-making procedures and bodies related to finding *potential* crises wherever they may arise. The financial intelligence networks described above fits into this category, in that it seeks to assess which emerging problems are ‘actionable’. The second category contains sense-making procedures and bodies for *actual* unfolding crises. They often involve marshalling expert groups for use in crisis. Examples include the Council's stakeholder advisory group on maritime security, which is expected to be ready when a maritime-related event takes place, and the counter-terrorism first response network, which convenes during an attack. As in most capacities inventoried in this report, we have very little information on whether these tools actually work in practice, and how well. But it is worth noting a key trend here, which becomes apparent when compared with previous analyses on EU sense-making (Boin, et al 2015): systems originally designed for information collection (e.g. largely about detection) have been 'enriched' with an analytical function (e.g. sense-making).

Decision-making

Decision-making is 'the selection of strategic decisions, joint decision-making, and formulating an effective strategy to implement the key decisions' (Transcrisis codebook, p. 11). In practice, we searched for capacities such as crisis rooms or decision-making protocols for use during a crisis.

Direct decision-making capacities for crisis management exist in only a few sectors. Those sectors correspond with issue areas in which the EU has a clear competence. Thus, during an animal health outbreak, key decisions must be made at the European institutions related to quarantine, for instance. Some aspects of air transport security involve Eurocontrol (not formally an EU body but closely related) issuing guidelines when a crisis hits, via its EACCC and Network Manager. In a major financial crisis, which is studied by a different sub-project within Transcrisis, the European Council will mobilize to coordinate a common response amongst member states and institutions like the European Central Bank.

But in most areas the EU's decision-making role is, at best, arms-length from the actual crisis. The EU's competences rarely allow it to intervene directly in a crisis. Thus, the ERCC has a variety of rapid decision-making protocols and an impressive information support system to match. Its three crisis rooms operate on a 24 hour/7 days a week basis. Decisions made here, however, relate mainly to the mobilisation of the EU's own assets—which are proportionally a small contribution to crisis response. The same applies to DG Santé's Health Emergency Operations Facility (HEOF). The Facility operates mainly to gain a situation awareness of a pandemic outbreak and to understand what EU member states are doing individually or bilaterally to manage a crisis. One respondent described HEOF's attempts as 'managing chaos' since DG Santé's role is not always self-evident. In the area of cyber crises, the 'EU Standard Operating Procedures for Cyber Events' involve a degree of decision-making but largely in terms of what EU capacities should be mobilized – whether demanded by outside crisis managers or not.

Coordination

Coordination involves 'identifying key partners in the response and facilitating collaboration between them' (Transcrisis codebook, p. 11). Here we searched for capacities related to coordination of crisis measures (e.g. coherence) as well as coordination of actors per se.

We found a plethora of coordination capacities, arguably because coordination is the very essence of the EU's role in crises (Boin et al. 2013). As argued above, the EU has few direct decision-making functions during crises. Rather, it is heavily concerned with coordinating itself (services, institutions) and *attempts* to coordinate national actors. We find that many of the capacities listed in this report are, in fact, coordinating in nature (even decision-making, which involves making decisions when and how to coordinate).

Our findings here fall into two categories, related to coordination before and during a crisis, respectively. Capacities used *before* a crisis are aimed at trying to assemble key actors, to educate on available resources, and to practice using relevant tools in advance of a crisis. Not all sectors engage in exercises, but they seem to be growing. The Council's IPCR (Integrated Political Crisis Response) is practiced once per year, under the leadership of the Council Presidency. Pandemic response plans are exercised on a fairly regular basis. And Cyber Europe is a bi-annual Pan-European cyber exercise that aims, amongst other goals, to practice crisis response collaboration with various actors – both vertically and horizontal.

Capacities for use *during* a crisis blend somewhat with the 'partial' decision-making capacities described above. As mentioned, most of what the EU considers decision-making capacities are actually coordination capacities according to the Transcrisis framework. Thus, the European Response Coordination Centre (ERCC), the IPCR, the Health Emergency Operations Facility (HEOF, in Luxembourg) and the European Aviation Crisis Coordination Cell (EACCC) are all sometimes considered 'decision platforms', but are more accurately described as coordination centres.

Moving beyond the decision-making vs. coordination debate, another reason that coordination efforts have grown in Brussels is the increasing number of actors involved in various crisis issue areas. The rise of new agencies, new member state officials, increased public-private relations, and new staff focused on crisis issues makes coordination more complicated than in previous years.

Meaning-making and Communication

Meaning-making refers to 'formulating a key message that offers an explanation of the threat [and] actionable advice' while Communication refers to 'effective delivery of the core message to selected audiences' (Transcrisis codebook, p. 11). We combined these categories for practical reasons; namely, both of these capacities tend to be centrally organised in media relations departments. For the Commission, this is the Spokespersons' Service located under the Commission President. The service has responsibility for media communication strategies across the Commission DGs. Our next stage of research will investigate crisis-related protocols in this area. For the moment, we have limited data here.

Communication capacities during a crisis include the effective delivery of a core message to selected audiences. For Transcrisis, this is a different kind of task from meaning making. We will investigate communication capacities alongside meaning making capacities in our next stage of research, focusing both on 'paper protocols' and on social media outreach strategies that can be used to communicate crisis messages.

Accountability

Accountability for the Transcrisis project involves 'rendering an explanation in a public forum of relevant decisions and strategies that were initiated before, during and after the crisis' (Transcrisis codebook, p. 11). Like meaning-making/communication, accountability is a task that does not differ greatly amongst issue areas. So we provide here a cross-sectoral assessment of accountability for the three main institutions under examination. This discussion also provides the basis for a paper on EU Crisis Management Legitimacy currently in preparation.

In the EU, accountability mechanisms are present but in varied forms. We can focus on three versions of accountability. Input-forms of accountability concern the relationship between citizens and those democratically chosen to represent them. National leaders taking decisions in the Council of Ministers and European Council are accountable to their respective national publics, for instance. Collectively, however, national leaders are not accountable to a European public since each represents only his/her respective citizens. Throughput versions of accountability concern how citizens can understand and hold to account the procedures and ways crises are handled. The EU machinery for acting on crises is not particularly transparent or easily comprehensible. Worse still, crisis-specific procedures often lead to improvisational processes and decision-making. In the EU, this means crisis decision-making is unlikely to follow the familiar Community Method of decision-making. Output forms of accountability concern holding leaders to account for their performance during crises. What decisions were taken, why and did they work? Here accountability mechanisms are stronger. First, the EU's institutional checks-and-balances systems encourage oversight and investigations over one another. The European Parliament takes seriously its role as 'watchdog' over other institutions, launching countless investigations. Second, the Brussels Press Corps is active and large – by some counts, the largest in the world – and can shine light and ask tough questions regarding crisis management performance.

Implications and Areas for Further Research

Our preliminary interpretation of the findings is as follows:

1. Most capacities relevant for managing crises reside in the largest administration within the EU's institutional landscape: The Commission. There are exceptions, including the Integrated Political Crisis Response (IPCR), which is administered from the General Secretariat of the Council and aims, with varying success, to draw in all EU institutions. The European Council itself has a very small secretariat – relying on the Council General Secretariat and, informally, the European Commission for most of its heavy lifting – but has a potentially powerful role in crisis decision-making. Thus, worth further exploring is the modest but noticeable accumulation of capacities outside of the Commission in both the Council of Ministers and the European Council, as well as in EU agencies (the latter covered by a separate Transcrisis sub-project). Interesting analytical questions include: do these developments follow a functional, bureaucratic, or political logic of accumulation?

2. Most capacities are sectoral-oriented. Very few operate across sectoral boundaries. Exceptions include the Council's IPCR and the Commission's ARGUS. Compared to previous findings in 2013 and 2015, cross-sectoral capacity building seems to have stalled. The Commission Secretariat General unit for cross-sectoral crisis coordination has changed name (from crisis coordination to business continuity), along with its emphasis. One might be forgiven for wondering whether old lessons will need to be relearned after the next crisis.

3. There is a difference in scope regarding EU detection/sense-making activities and EU decision-making/coordination activities. The former tend to focus on very specific threats, while the latter tends to cover a generic range. Examples of narrow detection activities include: the RAS-BICHAT and RAS-CHEM rapid alert systems (which differ only on whether terrorism is involved), the five different early warning and information sharing systems for different diseases (nominally aggregated in the Epidemic Intelligence Information System), and detection focused on the individual modes of Pan-European transport. Yet for decision-making and coordination, systems tend to be more generic. Thus, the ERCC claims a role as an 'all hazards' decision/coordination centre, and the IPCR has no specific threat orientation and is instead a decision platform for any contingency (although, as a side note, it is rarely used). Some of this can be explained by institutional affiliation and bureaucratic politics: the ERCC has maneuvered to become the main crisis hub for the Commission, while the IPCR's Council location explains its broad approach. Nevertheless, more exploration of this phenomenon is warranted.

4. A curious finding is the high number of capacities found in both detection and sense-making. Regarding detection, we surmise that creating detection and early warning capacities requires very little political authorisation from member states. Building such capacities is something the Commission can do largely as an administrative act. Moreover, political legitimation is easy: it seems like a 'good idea' to everyone. Contrast this with decision-making or coordination, which impacts upon national sovereignty and autonomy to a greater extent. These capacities are thus less well-developed. This hypothesis will be explored in a future paper.

   The rise of sense-making capacities, when compared to previous research in 2013 and 2015, is worth noting. Many of the tools and systems previously focused only on detection and early warning now contain an 'information enrichment' and analysis component. Systems that started as detection, threat mapping, and early warning – and then grew into sense-making systems – include the 'Network Manager' function in the Network Operations Portal for Eurocontrol, COPERNICAS for environmental threats, and ENSEMBLE, which monitors atmospheric problems. Why have such evolutions taken place? One hypothesis is cognitive: detection systems produce large quantities of data but not quality data. Policymakers saw the need for improvement, along the lines of crisis management theory's message that 'information does not equal understanding'. Another hypothesis is functional-bureaucratic: the overproduction of detection systems led to consolidation, which in turn demanded a functionalist response to organise the data more efficiently. The result was new functions for filtering, analysis and reporting to justify the continued existence of the system.

5. The 7-part framework for studying crisis management – detection, sense-making, decision-making, coordination, sense-making, communication, accountability – enabled a deeper understanding of EU capacities. It allowed for a refined categorisation of capacities previously described in broad strokes, like preparation or decision-making. Regarding preparation, being able to distinguish between detection and sense-making was quite revealing (see above). Regarding decision-making, the breakdown into decision-making and coordination offered the reminder that the EU actually does more coordination than decision-making.

   That said, the framework has some weaknesses. *First*, considerable subjective interpretation is needed in some areas. Are European Border Guard Teams, which assess crisis situations, a sense-making instrument or a coordinating activity, to cite one of many examples? *Second*, the framework lacks a category for material capacities used in crisis management. Emergency oil stocks, hazmat supplies, vaccine stockpiles, and rapid accommodation supplies are just some material capacities that find no easy 'home' in this framework. *Third*, although the framework claims to account for preparation activities, there is no obvious category for the EU's many crisis scenario exercises it undertakes. We placed these kinds of exercises into the 'coordination' capacity but they sit awkwardly there. *Fourth*, the framework does not account for the temporal aspects of crisis management preparation. The capacities found here generally fall into two categories: some focused on activities pre-crisis, and some activities focused after the onset of a crisis. The framework is mainly geared to capture the latter, for better or worse. *Fifth*, the framework, combined with how we operationalised it, emphasises concrete venues and technical instruments rather than social processes. This especially affects our ability to understand sense-making and meaning-making, tasks which are not well-captured by focusing only on tools and instruments.

6. The results here seem to validate the institutionalisation framework for analysis designed by Boin, Ekengren and Rhinard (2013b). Namely, there is a clear cycle that moves from informal practices to formal mechanisms. One of many examples is the informal information sharing system that once governed national officials responsible for cyber-attacks: it has recently turned into the CSIRT network. The process starts with a perceived problem, an experimental solution is designed, problems emerge with the original design, adaption takes place and over time the solution is perceived as 'legitimate'. This bears resonance to the 'institutionalisation of European governance' approach suggested by Sandholtz and Stone-Sweet (1998), although that project never examined EU crisis management.

7. Through our empirics, we discovered that the seven tasks explored through the Transcrisis project (from detection to accountability) can be divided into pre-crisis and mid-crisis activities. For instance, sense-making activities can be found directed towards horizon-scanning (pre-crisis), but also in terms of situation assessment (mid-crisis). The same goes for coordination. Some coordination activities are focused on 'getting ready' for a crisis and some are engineered for use during a crisis. Of course, the lines blend significantly here. The Transcrisis project officially looks only at preparation and response phases of crisis management, however, which means much of the pre-crisis activities we identified here are not accounted for by the framework.

8. Some larger questions emerge from this data. Taking a page from the literature on 'governmentality', one wonders the extent to which these capacities relate to two broader phenomena regarding the functioning of modern government. One is the way in which some of these capacities – detection and sense-making capacities, in particular – drive officials towards making decisions they might not otherwise have made. The EWRS and CIWIN systems, for instance, closely link detection with decision-making. Put crudely, governmentality suggests that modern technologies drive officials, rather than officials driving technology. A related phenomenon is the extent to which these activities serve to legitimise and validate the EU's existence, in a spiralling

logic by which the detection of risks demand responses, and the responses in turn provoke calls for more detection. This is related to Beck's claims we live in constructed 'risk society', of which the EU may be playing a central part.

We hasten to add that these observations are preliminary, and will be further developed following additional data collection and in regards to the project's main objectives. Those will feature in future deliverables and academic articles stemming from this Work Package.

References

Boin, A., Ekengren, M. & Rhinard, M., 2006. *Functional Security and Crisis Management Capacity in the European Union*, Stockholm: Swedish National Defence College, Acta B36.

Boin, A., Ekengren, M. & Rhinard, M., 2014. *Making Sense of Sense-Making : The EU's Role in Collecting , Analysing , and Disseminating Information in Times of Crisis*, Stockholm: Swedish National Defence College, Acta B Series, No. 44, 79 pages.

Boin, A., Ekengren, M. & Rhinard, M., 2013. *The European Union as Crisis Manager: Problems and Prospects*, Cambridge: Cambridge University Press.

Stone-Sweet, A., Fligstein, N. & Sandholtz, W., 2001. The Institutionalization of European Space. In A. S. Sweet, W. Sandholtz, & N. Fligstein, eds. *The Institutionalization of Europe*. Oxford: Oxford University Press.

Part I: European Commission Crisis Management Capacities

The Counter Terrorism Sector

Introduction

General Background

Due to the terrorist attacks in Europe lately, the EU has stepped up its efforts to counter terrorism. This is noticeable in, for example, the **European Agenda on Security from 2015** (where counter terrorism is one of three core priorities), the creation of the **European Counter Terrorism Centre** in early 2016, and intensified discussions with **The EU Counter Terrorism Coordinator** on how to improve the counter terrorism response of the EU, as well as intensified discussions with third countries on counter terrorist cooperation. During 2016 so far, the Coordinator has attended meetings with, for example, United Arab Emirates, Qatar and Jordania in order to strengthen cooperation on issues of foreign terrorist fighters and countering extremism. [1]

Generally, the development of many of the EU measures for countering terrorism has been a response to terrorist attacks. For example, the Eurojust was set up in the wake of 9/11. After the Madrid and London attacks the EU's counter terrorism strategy was published. After Charlie Hebdo in 2015, many Member States as well as the EU stated that new laws to combat terrorism will be adopted. [2]

Another example is the Task Force Fraternité, an investigation team within the European Counter Terrorism Centre located under Europol, with the objective to support primarily the investigations after the 2015 Paris attacks. As mentioned, the creation of The EU Counter Terrorism Centre is an answer to the increase of attacks in Europe lately. As Dimitris Avramopoulos, European Commissioner for Migration, Home Affairs and Citizenship, stated in connection to the launch of the Centre in January 2016; *"EU institutions responded swiftly and strongly to the terrorist attacks of last year and moved to augment the European Union's capacity to deal with the terrorist threat. As foreseen in the European Agenda on Security put forward by the European Commission, the establishment of the European Counter Terrorism Centre is a major strategic opportunity for the EU to make our collective efforts to fight terrorism more effective. I call on EU Member States to trust and support the European Counter Terrorism Centre to help it succeed in its important mission*".[3] One of the objectives of the EU is to enhance the connection between the Civil Protection Mechanism and protection of the civilian population against the effects of terrorist attacks, including CBRN. [4]

There is sometimes a conflict between counter terrorism measures and privacy. For example, in 2006, there was a data retention directive presented, requiring communication providers to storage of data

[1] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/
[2] http://www.cer.org.uk/insights/after-paris-what%E2%80%99s-next-eu%E2%80%99s-counter-terrorism-policy
[3] https://www.europol.europa.eu/content/ectc
[4] EU Plan of Action on Combating Terrorism, p. 64

about their costumers – a directive that has now been declared void by ECJ due to privacy aspects. Suggestions on expanding the use of personal data (for example flight passenger data) or increasing the efficiency of databases containing personal data (such as SIS) is often opposed because its possible implications on privacy of citizens. This is also why initiatives such as the Passenger Name Records (EU PNR) and the EU-US agreement on the Terrorist Finance Tracking Programme (TFTP) have been quite controversial. The solution to adopt the TFTP was eventually to add privacy clauses.[5]

Policy Background

After the terrorist attacks in Madrid 2004, the Council adopted the **Declaration on Combating Terrorism**. This also gave mandate to a revised Plan of Action to combat Terrorism, recalling the declaration on solidarity against terrorism (to jointly act and mobilize all available means (including military) if one of the member states is being attacked. For the purpose of informing preparation of the revised action plan, the following seven strategic goals were set up;

1. To deepen the international consensus and enhance international efforts to combat terrorism;
2. To reduce the access of terrorists to financial and economic resources;
3. To maximise the capacity within EU bodies and member States to detect, investigate and prosecute terrorists and to prevent terrorist attacks;
4. To protect the security of international transport and ensure effective systems of border control;
5. To enhance the capability of the European Union and of member States to deal with the consequences of a terrorist attack;
6. To address the factors which contribute to support for, and recruitment into, terrorism;
7. To target actions under EU external relations towards priority Third Countries where counter-terrorist capacity or commitment to combating terrorism needs to be enhanced.[6]

In relation to the European Chied's Police Task Force in Dublin in March 2004, it was concluded that Member States should have a coordinating body between police and intelligence regarding terrorism, and that Member States should have one **single contact point** for the EU Coordinator on Terrorism.[7]

In May 2004, the Council made the database of military and civilian capabilities relevant to the protection against terrorist attacks available to the Civil Protection Mechanism, as a part of the objective to enhance EU interconnection in order to improve preparedness, alerts and response across

[5] http://www.cer.org.uk/insights/after-paris-what%E2%80%99s-next-eu%E2%80%99s-counter-terrorism-policy
[6] EU Plan of Action on Combating Terrorism, p.4
[7] EU Plan of Action on Combating Terrorism, p. 40

all EU bodies.[8] To fully implement EU CBRN programmes (and the EU Health Security Strategy) was considered as an important measure of protection from terrorist attacks.[9]

- **EU Counter Terrorism Strategy**

Due to the identified need of a holistic counter-terrorism response, the EU Counter-Terrorism Strategy was adopted 2005. The strategy is focused on 4 main points;

- **Preventing** terrorism
- **Protecting** critical infrastructures and citizens from terrorist attacks
- **Pursuing** investigations and bringing terrorists to justice
- **Responding** by preparing for management of a terrorist attack, from response to recovery.[10]

- **European security strategy**

The EU Security Strategy was adopted in 2003 and reviewed in 2008, confirming its validity. It singled out 5 key threats, of which terrorism is one.[11]

- **Specific Programme: Prevention, preparedness and consequence management of terrorism (2007-2013)**

The Programme focused on fostering prevention and preparedness, especially by improving the protection of critical infrastructures. The programme also added consequence management as a component for enhanced crisis management coordination.

Based on the reports from the EU Counter Terrorism Coordinator on the issue of foreign fighters and returnees 2013, the JHA Council adopted 22 measures. In 2014 the Coordinator submitted progress reports on the implementation of the 22 measures. Moreover, many meetings with third country authorities were conducted in order to identify future cooperation opportunities. [12]

- **EU Strategy for Combating Radicalisation and Recruitment to Terrorism**

The EU Strategy for Combating Radicalisation and Recruitment to Terrorism was part of the broader EU Counter Terrorism Strategy and Action Plan. In 2014, the Council adopted a revision of the strategy due to the evolving trends of foreign fighters and lone actors.

- **A safer EU: police cooperation, and crisis management (2014)**

[8] EU Plan of Action on Combating Terrorism, p. 62
[9] EU Plan of Action on Combating Terrorism, p. 64
[10] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/index_en.htm
[11] http://www.eeas.europa.eu/csdp/about-csdp/european-security-strategy/
[12] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

- **Traceability of money transfers (2015)**
- **European Agenda on Security**

Due to the increasing complexity and number of threats, as well as the cross-border nature of these threats, the identified need for closer EU cooperation on all levels regarding was the background to the **European Agenda on Security**, published 2015.[13] Terrorism, cybercrime and organized crime are identified as the three core priorities for immediate action, and as they are cross border and interlinked, the EU-level is especially relevant for countering measures.

The Counter Terrorism Actions of the European Agenda on Security is as follows;

- Reinforcing Europol`s support functions by bringing together its anti-terrorism law enforcement capabilities in a European Counter-Terrorism Centre within Europol;
- Launching an EU Forum with IT companies to help counter terrorist propaganda and addressing concerns about new encryption technologies;
- Taking further measures to improve the fight against terrorism financing;
- Addressing any gaps in the response to incitement to hatred online; - Reviewing the Framework Decision on terrorism with a proposal in 2016;
- Re-prioritising the EU's policy frameworks and programmes for education, youth and culture;
- Focusing on the prevention of radicalisation in prisons, and developing effective disengagement/de-radicalisation programmes;
- Launching the RAN centre of excellence and extending anti-radicalisation work with Turkey, the Western Balkans, the Middle East and North Africa.[14]

- **Directive on PNR**

During December 2015 the Council approved (after years of negotiation) the controversial directive on the use of passenger name record (PNR) for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.[15]

- **Updated Directive on Combating Terrorism**

In December 2015, the Commission proposed an updated Directive on Combating Terrorism, including extended criminalization framework which goes in line with requirements of the UN Security Council Resolution 2178 (2014) and the Additional Protocol to the Council of Europe

[13] http://ec.europa.eu/dgs/home-affairs/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf
[14] The EU Agenda on Security, 2015, p.16
[15]Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 12

(CoE) Convention on the Prevention of Terrorism, signed on behalf of the EU on 22 October 2015.

- **Impact Assessment regarding updating the framework decision on terrorism**

An impact assessment by the Commission regarding updating the 2008 framework Decision on Terrorism is expected during 2016.[16]

- **Proposed upgrade of ECRIS**

In January 2016, the Commission proposed an upgrade of the Criminal Records Information System (ECRIS), which is used in order to exchange criminal records of EU citizens. The Council's approach on this will be expected in June 2016.[17]

Events and attacks

- **11 March 2004 Madrid, Spain**

2004 bombings of commuter trains in Spain killed 191 people and injured more than 1,800. The bombings were the deadliest terrorist attack in Spain's history.[18]

- **8 October 2004 Paris, France**

Ten people were injured when a parcel bomb exploded outside the Indonesian embassy in Paris.[19]

- **7 July 2005, London United Kingdom**

In London, at 8.50am on Thursday 7 July, three bombs exploded simultaneously, destroying sections of three different London Underground trains. The explosions killed 52 and injured over 700.[20]

- **15 March 2012 Montauban, France , 19 March 2012 Toulouse, France**

A gunman carried out a series of attacks that left seven people dead and two wounded in south-western France.

- **18 July 2012 Burgas, Bulgaria**

[16] EU Agenda on Security, 2015, p.14

[17] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 18

[18] http://edition.cnn.com/2013/11/04/world/europe/spain-train-bombings-fast-facts/

[19] https://www.theguardian.com/world/2004/oct/09/indonesia.france

[20] http://www.history.co.uk/study-topics/history-of-london/77-london-bombings

7 killed and 30 injured during bus suicide attack.[21]

- **24 May 2014 Brussels, Belgium**

Three people were killed and another was seriously injured in a shooting at the Jewish Museum of Belgium in Brussels.[22]

- **7 January 2015 Paris, France**

From January 7 to January 9, a total of 17 people are killed in attacks on the satirical magazine Charlie Hebdo, a kosher grocery store, and the Paris suburb of Montrouge.[23]

- **13 November 2015 Paris, France**

A series of coordinated terrorist attacks (shootings and bombings) in Paris, France and the city's northern suburb, Saint-Denis. Left 130 people dead and hundreds wounded.

- **22 March 2016 Brussels, Belgium**

Bombings at Brussels airport and a metro station in the city killed 32 people from around the world. Many more were injured in the attacks.[24]

- **14 July 2016 Nice, France**

On the evening of 14 July 2016, 84 people were killed and 303 injured when a 19-tonne cargo truck was deliberately driven into crowds celebrating Bastille Day on the Promenade des Anglais in Nice, France.

Institutional landscape

Eurojust

Eurojust aim to stimulate and improve the coordination of investigations and prosecutions as well as the cooperation between the Member States.[25]

Europol

Europol is the European Union's law enforcement agency. It has several expertise areas, among them counter terrorism. The European Counter Terrorism Center has been set up within the Europol structure during 2016.

[21] http://www.bbc.com/news/world-europe-18892336
[22] http://edition.cnn.com/2014/05/24/world/europe/belgium-jewish-museum-shooting/
[23] http://edition.cnn.com/2015/01/21/europe/2015-paris-terror-attacks-fast-facts/
[24] http://www.bbc.com/news/world-europe-35869985
[25] http://www.eurojust.europa.eu/about/background/Pages/mission-tasks.aspx

European Commission (HOME, JUST, DEVCO, FPI)

“The Commission's main role in the counter terrorism area is to assist EU State authorities in carefully targeted actions and initiatives, primarily within the PREVENT and PROTECT strands of the EU counter terrorism strategy. The Commission may also support EU States by approximating the legal framework, in full respect of the subsidiarity and proportionality principles.”[26]

EEAS

“Counter Terrorism as a matter of national security is mainly a Member Stated competence. EEAS focuses on the external dimension of CT in close coordination with the MS in the Council Working Group as well as with all relevant EU institutions involved. EEAS role is to coordinate CT external outreach and capacity building assistance to third countries by EU and MS, to ensure coherence and efficiency.”[27]

Justice and Home Affairs Council of the European Union

Works closely with the Counter-Terrorism Coordinator, who regularly submit progress report to the Council on the implementation of measures agreed by the ministers, as well as proposals for future work.[28]

Inventory

Detection

*VISA Information System (VIS)

By an IT system and infrastructure that links the national level systems with the central VIS system, the VISA information system allows Schengen states to exchange visa data. The VIS system is capable of fingerprint identification and verification, and assists in detecting suspected terrorism.[29] By facilitating checks and the issuance of visas and ensure identity of travelers, the VISA information supports prevention of terrorist attacks.[30]

*The Schengen Information System (SIS) II

SIS is an information system with the purpose of supporting law enforcement and external border control cooperation in Schengen States. SIS allows police and other authorities to find and to provide alerts on missing or wanted people and objects, but it also contains information on procedures when

[26] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/index_en.htm
[27] http://eeas.europa.eu/fight-against-terrorism/index_en.htm
[28] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/
[29] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm
[30] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

this object or person is found. Specialised national SIRENE Bureaux are point of contacts and coordinators for SIS-alert activities.[31] SIS II is the updated version of the original SIS, which became more connected to Europol. For example, SIS II allows Europol to cross-check information from its own communication channels, thus support Europol's role as an information-hub. During 2016, Europol's goal is to perform regular batch searches in SIS II, which will enhance its capability of cross-checking information from non-Schengen countries. However, Europol is not yet connected to VIS or Eurodac. [32]

*European Cybercrime Centre (EC3)

Since terrorism may have cyber components such as online radicalization, Member States can make use of Europol's cybercrime countering capabilities – including detection. The Europol's cybercrime capabilities are centered in the European Cybercrime Centre.

Europol Information System (EIS)

The Europol Information System aims to provide a reference system including offences, the individuals involved in the offences (for example foreign terrorist fighters) and other relevant information which is important for the investigations and fight against organized crime and terrorism. It supports both Member States individually and Europol as well as partners/third parties. Since its launch, there has been a continuous increase of inserted data into EIS, from 18 reported terrorist fighters during 2014 to 1131 during April 2015 and 1595 during the end of 2015.[33]

Working Group DUMAS

Working Group DUMAS was established in 2014 and is supported by Europol while the leadership is Italian. The working group's focus is on countering foreign fighter traveling. This includes for example traveler alert lists, best practice sharing and indicators for detection of foreign fighters travelling.[34]

Sensemaking

The European Explosive Ordnance Disposal Network (EEODN)

EEODN was established as a measure of the EU Action Plan on Enhancing the Security of Explosives, approved by the JHA ministers in 2008. It is a platform of information sharing between explosives and

[31] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/alerts-and-data-in-the-sis/index_en.htm
[32] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 15
[33] https://www.europol.europa.eu/content/page/europol-information-system-eis-1850
[34] Foreign Fighters and returnees: Implementation of the measures decided
by the JHA Council on 9-10 October 2014, p. 8

chemical, biological, radiological/nuclear (CBRN) and EOD experts in the EU, which aims to enhance knowledge and discuss threats of explosives and CBRN. The EEODN also arrange training sessions and conferences on the subject.[35]

*VISA Information System (VIS)

By an IT system and infrastructure that links the national level systems with the central VIS system, the VISA information system allows Schengen states to share information in order to support investigation of terrorist offences.[36]

*The Schengen Information System (SIS) II

SIS is an information system with the purpose of supporting law enforcement and external border control cooperation in Schengen States. SIS allows police and other authorities to find and to provide alerts on missing or wanted people and objects, but it also contains information on procedures when this object or person is found. Specialised national SIRENE Bureaux are point of contacts and coordinators for SIS-alert activities.[37] SIS II is the updated version of the original SIS, which became more connected to Europol. For example, SIS II allows Europol to cross-check information from its own communication channels, thus support Europol's role as an information-hub. During 2016, Europol's goal is to perform regular batch searches in SIS II, which will enhance its capability of cross-checking information from non-Schengen countries. However, Europol is not yet connected to VIS or Eurodac. [38]

*European Cybercrime Centre (EC3)

Since terrorism may have cyber components such as online radicalization, Member States can make use of Europol's cybercrime countering capabilities – including strategic analysis. The Europol's cybercrime capabilities are centered in the European Cybercrime Centre.

*Computer Network of the European Union Member States' Financial Intelligence Units (FIU.net)

The computer network of the European Union Member States' Financial Intelligence Units (FIU.net) is an intelligence platform which became embedded in Europol's financial intelligence and counter terrorism capabilities in the beginning of 2016. By integrating the network, Europol aims to boost the

[35] https://www.europol.europa.eu/latest_news/european-eod-network-eeodn-conference-and-training-warsaw-poland-25-28-october-2011

[36] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm

[37] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/alerts-and-data-in-the-sis/index_en.htm

[38]Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 15

fight against terrorism and organized crime in the EU, creating synergy effects between criminal and financial intelligence.[39]

*Eurojust

Eurojust is an EU agency, assisting and supporting Member States investigations and prosecutions and seeks to improve cooperation between the Member States in the fight against crime. Eurojust have experienced a continuous increase of registered terrorism cases since 2014, when 14 cases were registered compared to 41 cases in 2015. Information on ongoing prosecutions has increased from 180 (2014) to 217 (2015). However, Eurojust requests the Member States to increase the transmission of terrorist offences on a regular basis. [40]

*Radicalization Awareness Network (RAN)

The RAN is a network and a platform which brings together practitioners countering radicalization in Europe to share experiences, knowledge and peer review each other's practises. RAN was established in late 2015 and is financed by the Commission (who has set aside 25 million EUR between 2014-2017 for the purpose). The RAN Centre Of Excellence was established in October 2015. The Centre has meetings addressing counter terrorism in various areas linked to the RAN working groups. It also encourages academia to be part of its activities, and Member State authorities can apply for RAN support in terms of for example training, workshops and advice. Currently, the Commission is looking into the possibility to involve third states into RAN activities, where countries in the Africa and Middle East , Western Balkans and Turkey are of special interest. [41]

RAN is structured around 9 thematic working groups, driven by a Steering Committee (SC) chaired by the Commission. The SC includes the leaders of the working groups and the CoE.

Communication and Narratives working group (RAN C&N)

Countering extremist propaganda. [42]

Education working group (RAN EDU)

Countering readicalisation through education in schools. [43]

[39]Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 13

[40] European Council, Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing, 2015, p.16

[41]Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 34

[42] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[43] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

Youth, Families and Communities working group (RAN YF&C)

Supporting prevention of radicalization. [44]

Local authorities working group (RAN LOCAL)

RAN Working Group Local aims to promote local capacities to tackle radicalization, especially via multi-agency structures. It is a basis of interaction with other initiatives relevant for counter terrorism.[45]

Prison and Probation working group (RAN P&P)

Supports prevention initiatives in prison. [46]

Police and law enforcement working group (RAN POL)

Supports counter radicalization work of law enforcement and police. [47]

Health and Social Care working group (RAN H&SC)

Supports the work of discovering signs of radicalization in time, and support individuals in the risk zone of radicalization.[48]

*The Counter Terrorism Coordinator

In the wake of the Madrid attacks 2004, a EU counter terrorism coordinator position was established. Solana appointed Gilles de Kerchove to the position in 2007. [49] The role of the Counter Terrorism Coordinator includes;

- presenting policy recommendations and proposing priority areas for action to the Council, based on threat analysis and reports produced by the EU Intelligence Analysis Centre and Europol
- closely monitor the implementation of the EU counter-terrorism strategy
- maintaining an overview of all the instruments at the European Union's disposal, to regularly report to the Council and effectively follow up Council decisions[50]

[44] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[45] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 34

[46] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[47] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[48] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[49] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

[50] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

The Coordinator regularly report to the Council on issues an progress in the counter terrorism area.

*Europol

According to **the EU Counter Terrorism Coordinator** Europol's tools for countering terrorism have had a continuous increase in both use and contribution by the Member States, such as the database on European Foreign Terrorist Fighters. However, it is also states that less than half of the estimated actual number of Foreign Terrorist Fighters are reported to the database, and that some countries contributes more than others, why improvements are still considered necessary.[51] The aim of Europol is to enhance trust and awareness and utilizing capabilities among EU counter terrorism authorities.

*European Counter Terrorism Centre (ECTC)

The ECTC is situated under Europol and was launched in January 2016. It is a platform which is supposed to increase operational cooperation and information sharing among Member States. This includes, for example;

- Providing an information hub for counter terrorism for law enforcement authorities
- Expertise for investigations
- Strategic advise on, for example, use of social media for radicalization. [52]

EU Internet Referral Unit (IRU)

Radicalization online is a problem which the EU is taking seriously. The Internet Referral Unit, located at Europol and part of the ECTC, identifies and perform referrals and removals of items with violent/extremist content. It was established in July 2015, and has gotten contributions from almost all Member States so far. The proactive work of IRU demands close cooperation from Member States, so that the volume of referrals can increase. This includes for example national contact points of IRU, which a few Member States has not yet established. The objective of IRU for 2016 is that it will develop social media monitoring, develop capabilities to "decipher" jihadist networks, develop a Europol Platform of Experts in order to enhance contacts with academia and research and further enhance and build the relationship with the private sector (including "Joint Action Days").[53]

EU Internet Forum

The EU Internet Forum is a private-public cooperation framework, which brings together representatives from the internet industry, Europol, The EU Counter Terrorism Coordinator, The Parliament and EU Interior Ministers. It aims to enhance discussions on how to combat online

[51] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 15
[52] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 13
[53] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 35

radicalization and protect citizens from terrorism exploitation.[54] The EU Internet Forum is one of the key commitments from the European Agenda on Security from 2015. In December 2015, the Commission held the first Internet Forum meeting, discussing and agreeing on the importance of effective mechanism for private-public cooperation to efficiently and swiftly remove terrorist content online, and also to counter terrorist narratives. The participants also agreed on using the umbrella of the EU IT Forum for synergy effects in the counter terrorism work. Commissioner for Migration, Home Affairs and Citizenship, Dimitris Avramopoulos said:

"Terrorists are abusing the internet to spread their poisonous propaganda: that needs to stop. The voluntary partnership we launch today with the internet industry comes at the right time to address this problem. We want swift results. This is a new way to tackle this extremist abuse of the internet, and it will provide the platform for expert knowledge to be shared, for quick and operational conclusions to be developed, and powerful and credible voices to challenge extremist narratives."[55]

The First Response Network

The First Response Network was adopted in 2007 by the JHA Council of Ministers. It consists of EU Member States counter-terrorist experts which can be mobilized during a serious terrorist attack in Europe. When mobilized, the team will, under the coordination of Europol, use Europol's operational centre and provide experts with advice during an attack.[56]

Decisionmaking

Coordination

*European Counter Terrorism Centre (ECTC)

In major terrorist attacks, the ECTC is supposed to contribute to a coordinated reaction. Its focus lies in sharing expertise and intelligence on terrorism, especially on terrorism financing (supported by TFTP and FIU.net), counter foreign fighters, online radicalization, and enhancing efficiency of international cooperation on counter terrorism. Member States also has the possibility to second experts to the center in order to support investigations, of which the Task Force Fraternité is an example. In connection to the ECTC, tools like SIENA and EIS will be used for sensitive information

[54] http://europa.eu/rapid/press-release_IP-15-6243_sv.htm
[55] http://europa.eu/rapid/press-release_IP-15-6243_sv.htm
[56] https://www.europol.europa.eu/latest_news/europol-responds-attacks-norway-mobilising-eu-first-response-network

exchange of counter terrorism intelligence.[57] Included in the tasks of the ECTC is to provide operational support, coordination and expertise during a terrorist attack, such as;

- Direct and immediate on-the-spot support
- Emergency Response Team (EMRT)
- Live investigation support
- Incident response and coordination

*The Counter Terrorism Coordinator

In the wake of the Madrid attacks 2004, a EU counter terrorism coordinator position was established. Solana appointed Gilles de Kerchove to the position in 2007. [58] The role of the Counter Terrorism Coordinator includes to;

- coordinate the work of the Council in combating terrorism
- coordinate with the relevant preparatory bodies of the Council, the Commission and the EEAS and sharing information with them on his activities[59]

The Coordinator regularly report to the Council on issues an progress in the counter terrorism area.

Prüm

Prüm is a data exchange mechanism, deriving from a Council decision in 2008. It allows Member States to mutually access forensic biometric databases, which includes for example fingerprints and DNA. It also allows Member States to access vehicle registration data in order to counter-terrorism.[60]

*Eurojust

Eurojust is an EU agency, assisting and supporting Member States investigations and prosecutions and seeks to improve cooperation between the Member States in the fight against crime. Eurojust have experienced a continuous increase of registered terrorism cases since 2014, when 14 cases were registered compared to 41 cases in 2015. Information on ongoing prosecutions has increased from 180 (2014) to 217 (2015). However, Eurojust requests the Member States to increase the transmission of terrorist offences on a regular basis. The agency both supports Joint investigation Teams in terrorist cases, and organizes coordination centres and meetings on terrorism cases.[61]

[57] https://www.europol.europa.eu/content/ectc

[58] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

[59] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

[60] European Council, Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing, 2015, p.16

[61] European Council, Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing, 2015, p.16

Meaningmaking/Communication

*The Counter Terrorism Coordinator

The role of the Counter Terrorism Coordinator includes;

- presenting policy recommendations and proposing priority areas for action to the Council, based on threat analysis and reports produced by the EU Intelligence Analysis Centre and Europol
- maintaining an overview of all the instruments at the European Union's disposal, to regularly report to the Council and effectively follow up Council decisions
- improving communication between the EU and third countries in this area[62]

Secure Information Exchange Network Application (SIENA)

The Secure Information Exchange Network Application (SIENA) is a tool ran by Europol for exchanging information between Member States. In 2014, 14 EU Member States had connected its counter terrorism authorities to the network, and in 2015 a dedicated counter terrorism area in SIENA was launched, allowing direct communication between counter terrorism authorities in EU but also third parties such as Canada, Australia and the US. SIENA replaced the Police Working Group on Terrorisms (not an EU-WG) communication system and 2016, all Police Working Group on Terrorism-countries were connected to SIENA.[63]

Accountability

RAN Remembrance of Victims of Terrorism working group (RAN RVT)

RAN RVT works with victims of terrorism in order to utilize their experiences for countering radicalization. [64] By maintaining a network of organizations of victims, and keeping up remembrance ceremonies (such as the European Day of Remembrance of Victims of Terrorism 11 March), RAN RVT aim to draw on and transmit the experiences of victims of terror (both targets and those who have lost a relative) in order to counter radicalization. An example of the work of the RAN RVT is the Handbook of victim experiences shared, which is based on the contributions from experts, organizations, victims and practitioners during the RAN VVT-meetings.[65]

[62] http://www.consilium.europa.eu/en/policies/fight-against-terrorism/counter-terrorism-coordinator/

[63]European Council, Enhancing counter terrorism capabilities at EU level: European Counter Terrorism Centre (ECTC) at Europol and counter terrorism related information sharing, 2015, p.6

[64] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/index_en.htm

[65] http://ec.europa.eu/dgs/home-affairs/what-we-do/networks/radicalisation_awareness_network/about-ran/ran-rvt/index_en.htm

Task Force Fraternité (part of the ECTC)

Task Force Fraternité was established after the Paris 2015 attacks as an investigation team of the ECTC. By investigating and performing analysis of the attacks, the Task Force identified important lessons from the attacks and pin pointed gaps in counter terrorism intelligence as well as policy implications.[66]

The EU Bomb Data System (EBDS)

The EBDS consists of two databases for information exchange between experts regarding incidents, one focuses on explosives and the other CBRN incidents. In the database, experts may share experiences, discuss and share thoughts and lessons learned from incidents. It is mainly for EU authorities but non EU countries may be included if they have cooperation agreements with the EU.[67]

[66] Report from the EU counter terrorism coordinator to the council, 4 march 2016, p. 5

[67] http://ec.europa.eu/dgs/home-affairs/financing/fundings/projects/stories/ebds_en.htm

The Civil Protection Sector

Introduction

General Background

The EU is committed to support populations affected by natural or man-made disasters, both inside and outside the EU. The main instrument for the EU to provide civil protection assistance is the Civil Protection mechanism, established in 2001 to achieve a faster and more coordinated response to crises/disasters which overwhelms the response capacity of the country affected.[68] The Civil Protection Financial Instrument finances the Civil Protection Mechanism, and according to DG ECHO *"The Community Civil Protection Mechanism and the Civil Protection Financial Instrument together cover three of the main aspects of the disaster management cycle – prevention, preparedness and response. The Mechanism itself covers response and some preparedness actions, whereas the Financial Instrument enables actions in all three fields."*[69]

The objectives of the Civil Protection Mechanism are to;

- Strengthen cooperation between the Union and Member States in the field of civil protection
- Improve effectiveness of prevention, preparedness and response to natural and man-made disasters
- Pool resources and civil protection capabilities of participating states that can be requested in the case of an emergency[70]

The civil protection assistance could consist of, for example, coordination of efforts, delivery of civil protection assets, monitoring or deployment of expert teams to a crisis area.[71] The Directorate-General for European Civil Protection and Humanitarian Aid Operations (ECHO) is the responsible DG in the Commission, and has two main departments (brought together in 2010); humanitarian aid and civil protection. These are under the responsibility of the Commissioner for Humanitarian Aid and Crisis Management; Christos Stylianides. ECHO has a global network of field offices. Depending on type of disaster, ECHO works closely with relevant agencies - such as European Maritime Safety Agency (EMSA) in the case of maritime pollution disasters. The Mechanism currently has 6 members besides all 28 Member States of the EU (Serbia, Norway, the former Yugoslav Republic of Macedonia, Turkey, Montenegro and Iceland).[72] Since disasters are often borderless, the EU-level is, according to the Commission, especially suitable to provide coordination and avoid duplication of

[68] http://ec.europa.eu/echo/who/about-echo_en
[69] http://ec.europa.eu/echo/files/civil_protection/civil/prote/legal_texts.htm
[70] https://www.exchangeofexperts.eu/EN/Programme/UCPM/UCPM_node.html
[71] http://ec.europa.eu/echo/what/civil-protection_en
[72] http://ec.europa.eu/echo/what/civil-protection/mechanism_en

efforts during a crisis situation.[73] In recent years there has been a greater focus on prevention and preparedness measures, to support the improvement of Member States abilities to cope with disasters.[74]

Policy Background

The two main, complementary, legislative texts/pillars which regulates European civil protection;

- Council Decision 2007/779/EC, Euratom establishing a Community Civil Protection Mechanism (recast)
- Council Decision establishing a Civil Protection Financial Instrument (2007/162/EC, Euratom)

In relation to these, there has been 3 Commission decisions; - (2007/606/EC, Euratom) on transport rules and (2008/73/EC, Euratom) + (2010/481/EU, Euratom) on implementation of the modules concept.

Other important policy documents regarding civil protection are **the Commission Communication on Reinforcing the Union's Disaster Response Capacity** and **the Communication on strengthening Early Warning Systems in Europe**, both adopted in 2007. [75]

Earlier crises/incidents

The EU order disasters in two main categories, man-made (such as industrial and chemical accidents, marine pollution, terrorist attacks and war) and natural disasters. The latter is the most common type of disasters occurring in Europe. [76] Since 2001 when the Civil Protection Mechanism was launched, there have been more than 200 requests for assistance (including requests from countries outside the EU). [77] The EU has assisted in major disasters around the world, including typhoon Haiyan that hit the Philippines (2013), the floods in Serbia and Bosnia and Herzegovina (2014) – in which 23 participating states offered assistance, the Ebola outbreak (2014) – in which the OAS requested help and got rapid deployment of experts and supplies as well as medical evacuations, the conflict in Ukraine (since 2014), the earthquake in Nepal (2015) - in which the EU sent an expert team as well as

[73] http://ec.europa.eu/echo/who/about-echo_en
[74] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf
[75] http://ec.europa.eu/echo/files/civil_protection/civil/prote/legal_texts.htm
[76] http://ec.europa.eu/echo/files/civil_protection/vademecum/menu/1.html#diseur
[77] http://ec.europa.eu/echo/what/civil-protection_en

emergency supplies, and the refugee crisis in Europe – in which participating states sent supplies and material.[78] [79]

Forest fires are among the most common natural disaster incidents, causing the Mechanism to be activated 55 times since 2007 (however including alert and monitoring requests). For example, during 2014 the Mechanism was activated for Sweden and Norway, and a request was made by Greece in 2015, which activated an asset deployment of firefighting planes from the EU civil protection voluntary pool. Moreover, the satellite services of the Commission have been used several times in cases of forest fire. [80]

Just like in other crisis management sectors, institutional development has to some extent been a result of crises. For example, the 2002 floods of Elbe and Danube-rivers made clear the lack of early warning systems regarding floods in Europe. It also made clear the difficulty of managing a coherent response and aid-planning when information was lacking and fragmented. In the wake of these events, the Commission initiated the European Flood Awareness System (EFAS). [81]

Institutional landscape

The European Commission's Humanitarian Aid and Civil Protection department (ECHO)

Commission's Institute for Environment and Sustainability (IES)

The Joint Research Centre (JRC)

Inventories

Detection

* The Emergency Response Coordination Centre (ERCC)

The Emergency Response Coordination Centre (ERCC) is the operational hub of the Civil Protection Mechanism. Among its tasks are;

- The (non-stop) monitoring and mapping of emergencies and disasters around the world.
- The collection of real time information on disasters.

[78] http://ec.europa.eu/echo/what/civil-protection_en
[79] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf
[80] http://ec.europa.eu/echo/what-we-do/civil-protection/forest-fires_en
[81] https://www.efas.eu/about-efas.html

- The enabling of a quick response to both natural and man-made disasters should the Mechanism be activated.[82]

The Common Emergency Communication and Information System (CECIS)

The web-based alert/early warning system called “The Common Emergency Communication and Information System (CECIS) allow rapid information exchange between ERCC & Member States. [83]

The Global Disaster Alerts and Coordination System (GDACS)

The Global Disaster Alerts and Coordination System (GDACS) is a rapid alert system developed by the Joint Research Centre (JRC) which provides access to disaster information systems (and coordination tools) worldwide in order to achieve a faster response in the very first stages of a potential major disaster. It is applied worldwide and commonly used by both the UN and the EU. The JRC is responsible for establishing partnerships with hazard monitoring organizations all over the world, which provides the base for GDACS services. An advisory group consisting of various actors (from scholars to practitioners of various kinds related to disaster management) manages the GDACS development, with the The Activation and Coordination Support Unit (ACSU) in the United Nations Office for Coordination of Humanitarian Affairs (OCHA) as secretariat. [84]

Among the tasks of the GDACS are;

- Rapid alerts in relation to major disasters
- Guideline development for disaster information exchange.
- Providing disaster management coordination platform (Virtual OSOCC)
- Provides disaster maps/satellites.
- Provides weather forecasts (SARWeather) in relation to disaster analysis.

GDACS has about 14.000 users worldwide (disaster managers). Its automatic alerts and impact estimations are especially helpful in the first phase of disaster management. Moreover, it supports information exchange and therefore coordination between international responders to a disaster which reduces the risk of duplication of efforts or gaps in response.[85]

[82] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/ERC_en.pdf
[83] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf
[84] http://portal.gdacs.org/about
[85] http://portal.gdacs.org/about

* European Flood Alert System (EFAS)

The Flood Alert System (EFAS) is a monitoring system fully operational since 2012. It provides early warnings to its national partners as well as the ERCC. EFAS is developed by the Commission's Institute for Environment and Sustainability (IES) and is part of COPERNICUS Initial Operations (which supports the Civil Protection Mechanism). [86] It consists of four main centres (the operational management of them is outsourced to Member State organization);

1. EFAS Computational centre (hosting the EFAS Information System Platform and do forecasts)
2. EFAS Dissemination centre (perform daily analysis, provides information to the ERCC)
3. EFAS Hydrological data collection centre (performs water level data collection)
1. EFAS Meteorological data collection centre (collects meteorological data) [87]

Among the tasks of EFAS are;

- Provide early warnings in order to give time for preparedness measures.
- Provide information to national services.
- Provide information to the ERCC about upcoming and ongoing floods.[88]

*European Forest Fire Information System (EFFIS)

Established by the Commission, EFFIS support the fire-disaster management services in the EU. This includes forecasts on hazards, risk-areas and hot-spots.[89]

In 2015, EFFIS was incorporated under the umbrella of COPERNICUS Emergency Management Services.[90]

Meteoalarm

Meteoalarm provides early alerts of weather with the potential to cause disasters, such as heavy rain, forest fires, extreme cold, thunderstorms, etc. The service provides updated maps of affected areas and the estimated possible impact of weather as well as expected time-horizons for weather events. It includes both national and regional warnings.[91]

*COPERNICUS Emergency Management Service

Copernicus (previously Global Monitoring for Environment and Security - GMES) is an EU programme (implemented by the Commission) aimed at developing European information services

[86] http://ec.europa.eu/echo/what/civil-protection/monitoring-tools_en
[87] https://www.efas.eu/
[88] https://www.efas.eu/about-efas.html
[89] http://forest.jrc.ec.europa.eu/effis/
[90] http://forest.jrc.ec.europa.eu/effis/about-effis/
[91] http://www.meteoalarm.eu/about.php?lang=en_UK

based on satellite Earth Observation and in situ (non space) data. Copernicus aims to both monitor and forecast the environment situation on land, sea and in the air in order to improve safety of EU citizens.[92]

*Copernicus Rapid Mapping

Copernicus maps and monitors all kinds of emergency situations through satellite and open data source information. The information drawn from Copernicus might be used by various disaster management actors and be helpful in crisis decision making processes as well as geospatial analysis. It covers all crisis management phases. [93] There are three kinds of maps offered by the "Rapid Mapping" service of Copernicus, which is especially helpful in the response phase of a disaster;

- Reference Maps
- Delineation Maps (providing an assessment of the event extent)
- Grading Maps (providing an assessment of the damage grade and its spatial distribution). [94]

Sensemaking

*European Flood Alert System (EFAS)

The Flood Alert System (EFAS) is a monitoring system fully operational since 2012. It provides early warnings to its national partners as well as the ERCC. EFAS is developed by the Commission's Institute for Environment and Sustainability (IES) and is part of COPERNICUS Initial Operations (which supports the Civil Protection Mechanism). [95] It consists of four main centres (the operational management of them is outsourced to Member State organization);

4. EFAS Computational centre (hosting the EFAS Information System Platform and do forecasts)
5. EFAS Dissemination centre (perform daily analysis, provides information to the ERCC)
6. EFAS Hydrological data collection centre (performs water level data collection)
2. EFAS Meteorological data collection centre (collects meteorological data) [96]

Among the tasks of EFAS are;

- Provide information to national services.
- Provide information to the ERCC about upcoming and ongoing floods.[97]

[92] http://emergency.copernicus.eu/mapping/ems/what-copernicus
[93] http://emergency.copernicus.eu/mapping/ems/service-overview
[94] http://emergency.copernicus.eu/mapping/ems/service-overview
[95] http://ec.europa.eu/echo/what/civil-protection/monitoring-tools_en
[96] https://www.efas.eu/
[97] https://www.efas.eu/about-efas.html

*European Forest Fire Information System (EFFIS)

Established by the Commission, EFFIS support the fire-disaster management services in the EU and updates the Commission and European Parliament with common situational pictures on wildland fires in Europe. This includes;

- Current situation (forecasts, hazards, risk-areas and hot-spots).
- Fire news (media reports on wildland fires).
- Mobile app EFFIS. [98]

In 2015, EFFIS was incorporated under the umbrella of COPERNICUS Emergency Management Services. EFFIS has a network of experts called "The Expert Group on Forest Fires", including experts from 43 countries. During the initial phase of a fire, EFFIS performs rapid damage assessments, which is shared through the "Current situation" viewer.[99]

*The Civil Protection Mechanism

Within the Mechanism, Member States share their national risk assessment and share information about their risk management capabilities. The Commission supports and gives guidance to Member States individually and coordinates good practices exchange as well as voluntary peer reviews of national risk management plans.[100] In relation the Mechanism, the EU is funding transport and logistics of assistance. [101]

*The Emergency Response Coordination Centre (ERCC)

The ERCC is the operational centre of the Civil Protection Mechanism with a constant preparedness to coordinate an EU response to disasters. It monitors and collects information on disasters or hazards, analyzes that information and plan response activities such as deployment of expert-teams or needed equipment (from the voluntary pool). [102]

Decisionmaking

*The Emergency Response Coordination Centre (ERCC)

Besides preparation and planning, the ERCC ensures operational capacity during a disaster (when the Civil Protection Mechanism is activated). The ERCC was created in 2014, replacing/merging the Monitoring and Information Centre (MIC) as well as the ECHO crisis room. As the operational hub of the Civil Protection Mechanism, the ERCC provides around-the-clock, continuous emergency

[98] http://forest.jrc.ec.europa.eu/effis/
[99] http://forest.jrc.ec.europa.eu/effis/about-effis/
[100] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
[101] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf
[102] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf

management, and has the capacity to manage several ongoing emergencies in different time zones at the same time.[103] The ERCC is equipped with several workstations for specialized staff, and provides 24/7 crisis rooms. In order to be able to respond quickly to emergencies, it has pre-positioned teams ready to intervene and support where it is needed, both EU internally and externally. [104]

European Emergency Response Capacity (EERC)

The EERC is a voluntary pool connected to the Civil Protection Mechanism. It is considered as one of the major innovations in the Mechanism, allowing a faster, better and more coordinated response to disasters. It consists of pre-committed capacities/assets which can be deployed in case of a disaster. This significantly reduces time in response-activities from the EU-level. The Commission and Member States continuously develop criteria in order to ensure the quality of assets in the pool, especially in terms of interoperability. To this end, civil protection exercises, training and workshops are conducted to improve coordination and quality of civil protection teams in the pool. Moreover, EU financially supports transport of these teams in case of activation. [105]

European Medical Corps (EERC)

Part of the EERC is the European Medical Corps (EMC) which is a pool especially for medical/health experts ready to be deployed in case of emergency. The EMC improves response capacity in disasters with health aspects, and is the European contribution to the WHO's "Global Health Security Workforce.[106] By January 2016, nine Member States have already offered their specialised units to the European Medical Corps (Belgium, Luxembourg, Spain, Germany, the Czech Republic, France, the Netherlands, Finland, Sweden) and to date, two deployments of the European Medical Corps have been carried out, both in the context of the European response to the Ebola crisis. [107]

Coordination

ECHO civil protection exercises

ECHO funds various civil protection exercises every year (from modules/table-top to full-scale). Exercises are considered essential in order to enable civil protection teams to perform in a fast and coordinated manner during a crisis and to test or consolidate concepts and procedures of the Civil Protection Mechanism. The Commission releases call for proposals/tenders for exercise management

[103] http://erccportal.jrc.ec.europa.eu/About-ERCC

[104]http://www.europarl.europa.eu/RegData/bibliotheque/briefing/2013/130708/LDM_BRI(2013)130708_REV1_EN.pdf

[105] http://ec.europa.eu/echo/what/civil-protection/mechanism_en

[106] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf

[107] http://ec.europa.eu/echo/what-we-do/civil-protection/european-emergency-response-capacity_en

every year. While module or full-scale exercises is considered especially good for improving coordination and testing response capacity, table-tops is considered especially good for providing training and improvement of key people in civil protection contexts. Also, lessons learned from exercises gives valuable feedback for further improvement of civil protection management.[108]

EU Exchange of Experts programme

The EU Exchange of Experts Programme is part of the Civil Protection Mechanism, aiming to train experts to become more coordinated and improve their disaster response skills. The programme is built so that participating civil protection experts will exchange knowledge, best practices and techniques. [109] The duration of an exchange goes from a few days to two weeks. Experts might apply for the programme or be invited by a host organization to, for example, attend workshops, participate in exercises and attend conferences.[110]

*The Emergency Response Coordination Centre (ERCC)

As previously mentioned, the ERCC is the operational centre of the Civil Protection Mechanism with a constant preparedness to coordinate an EU response to disasters. The centre plans response activities such as deployment of expert-teams or needed equipment (from the voluntary pool). Its task as coordinator also make the ERCC contact point for the Integrated Political Crisis Response framework, as well as contact point in case of activation of the EU Solidarity Clause. In order to function as a coordinator of disaster response efforts, the ERCC works with Member State civil protection authorities. [111] Pre -positioned civil protection modules from Member States makes it possible for the ERCC to activate and deploy civil protection expert teams and equipment in a short notice. [112]

Meaningmaking/ Communication

*European Forest Fire Information System (EFFIS)

Established by the Commission, EFFIS support the fire-disaster management services in the EU and updates the Commission and European Parliament with common situational pictures on wildland fires in Europe. This includes;

- Fire news (media reports on wildland fires).
- Mobile app EFFIS. [113]

[108] http://ec.europa.eu/echo/what/civil-protection/simulation-exercises_en
[109] http://ec.europa.eu/echo/what/civil-protection/experts-training-and-exchange_en
[110] https://www.exchangeofexperts.eu/EN/Programme/Programme/programme_node.html
[111] http://ec.europa.eu/echo/files/aid/countries/factsheets/thematic/civil_protection_en.pdf
[112] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
[113] http://forest.jrc.ec.europa.eu/effis/

Vademecum web page

Vademecum is a website containing information on disaster measures taken by Member States and at the EU-level. It contributes to creating a common situational picture and is especially aimed towards civil protection professionals at all levels in the EU as well as NGO's and volunteers.[114]

NexT

NexT is a newsletter targeted towards civil protection experts and professionals in order to share information about civil protection. It is issued twice a year, and mainly focuses on matters of training and exercises in civil protection. Moreover, it suggests participation opportunities of various activities related to the Mechanism.

Accountability

*Copernicus Recovery Mapping

Risk and Recovery Mapping consists of the on-demand provision of geospatial information in support of Emergency Management activities not related to immediate response. This applies in particular to activities dealing with prevention, preparedness, disaster risk reduction and recovery phases. There are three broad product categories: Reference Maps, Pre-disaster Situation Maps and Post-disaster Situation Maps.[115]

*European Forest Fire Information System (EFFIS) post fire assessments

The monitoring service of EFFIS covers identification of hazards as well as assessment of post-fire damages. The module covering the last phase of management includes;

- Land cover damage assessment
- Emissions Assessment and Smoke Dispersion,
- Potential Soil Loss Assessment, and
- Vegetation Regeneration.

EFFIS is moreover supported by the "Fire Database" – entailing recorded information on previous fire accidents and disasters provided by the EFFIS network countries. [116]

[114] http://ec.europa.eu/echo/files/civil_protection/vademecum/index.html
[115] http://emergency.copernicus.eu/mapping/ems/service-overview
[116] http://forest.jrc.ec.europa.eu/effis/about-effis/

The Solidarity Fund

The solidarity fund supports management of the consequences of a major disaster. Through the solidarity fund, emergency services to deal with the short term restoration, damage control and peoples immediate needs can be mobilized quickly.[117]

[117] http://www.welcomeeurope.com/european-funds/solidarity-fund-483+383.html#tab=onglet_details

The Cybersecurity Sector

Introduction

General background

Despite the fact that cyber incidents are common, there have been few examples of cyber *crises* in the EU to this date. European Agency for Network and Information Security (ENISA) defines a cyber crisis as "an event or a series of events, natural or man-made, declared as such by a country. A multinational cyber crisis is where the causes or impact concern at least two countries". [118] This vague definition highlights the current difficulty to frame what a cyber crisis is as well as the lack of common terminology and understanding in the field of cybersecurity in the EU. The one event in the EU commonly referred to as a cyber crisis is the cyberattacks on Estonia 2007.[119] Cyber crises, or the possibility of such, are not just a new phenomenon but also a tremendously complex one. Cyber is, by its nature, transboundary. It transcends physical, non-physical, geographical and sectorial borders. The internet infrastructure itself is an abstract combination of physical elements and non-physical elements such as software, networks, services, protocols, plus human elements and operators. Failure in any part of the core components may spark an incident which might also spread fast through the borderless nature and connectivity of internet infrastructure. [120] Meanwhile, the threat from cybercrime has grown as more and more of society (including pay systems) moves to the digital domain.[121] The stakes get even higher as online economy also makes cyber key for the economic wellbeing and internal market of the EU.[122]

In conclusion, the borderless nature of cyber makes the cybersecurity-sector hard to capture. Cyber is entangled in all parts of society relying on online services, and therefore cybersecurity touches upon a society as a whole, involving everything from individuals and businesses to governments – individually as well as collectively. Therefore, cybersecurity efforts at the EU-level works in a number of fronts – from ensuring online privacy , promoting digital trust and battling cybercrime to funding research, enhance critical infrastructure protection and increase EU/international cybersecurity cooperation and coordination. [123]

Cybersecurity as well as privacy online are currently among the political priorities of the European Commission, and the Commission has continuously increased its cybersecurity efforts, especially

[118] https://www.enisa.europa.eu/news/enisa-news/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa

[119] ENISA, Report on Cyber Crisis Cooperation and Management, 2014, p. 36

[120] Threat Landscape and Good Practice Guide for Internet Infrastructure, 2015, p.1

[121] https://www.europol.europa.eu/ec3

[122] https://ec.europa.eu/digital-single-market/node/39826

[123] https://ec.europa.eu/digital-single-market/node/39826

since the launch of the EU Cybersecurity Strategy 2013 – including legislation, network activities and investments in research.[124]

Policy Background

During 2009, the 'Communication on Critical Information Infrastructure protection (CIIP)' was adopted the European Commission, setting the basic framework and action points for enhanced cybersecurity throughout the Union. It included both preventive and reactive measures, ranging from preparedness and prevention through detection and response as well as mitigation and recovery. The activities fell under or in parallel to the European Programme for Critical Infrastructure Protection (EPCIP).[125]

Following up on this initial framework, the Commission published the Communication on CIIP on "Achievements and next steps: towards global cyber-security" during 2011. In relation to this, the Commission highlighted the importance of a common, cooperative European response to cyber threats and risks.[126]

In June 2012, based on the results of discussions held in two Ministerial Conferences on CIIP, The European Parliament Resolution on "Critical Information Infrastructure Protection: towards global cyber-security" was published, including recommendations and objectives for continuous strengthening of cybersecurity within the EU.[127]

Based on the identified need of further clarifying roles, responsibilities and the EU vision regarding cybersecurity, the EU Cybersecurity Strategy was adopted during 2013, accompanied by the Commission's Proposal for the NIS-directive aiming to improve the overall EU cybersecurity by setting minimum NIS requirements for Member States. After preparatory work by the **Working Group on Telecommunications and the Information Society (WP Tele)**, The Council conducted a first orientation debate on the proposed directive in June 2013.

After several trilogue-meetings between 2014 and 2015, discussing and debating the Proposal, the European Parliament and the Council reached an agreement on the main principles of the NIS-directive during June 2015. In December 2015, an informal deal was struck with the European Parliament about the Directive, and during May 2016, the Council confirmed the agreement. During August 2016, the NIS-directive is expected to formally enter into force.[128]

[124] https://ec.europa.eu/digital-single-market/en/cybersecurity-privacy

[125] Communication on Critical Information Infrastructure protection (CIIP), 2009, p.3

[126] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

[127] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

[128] http://www.consilium.europa.eu/en/policies/cyber-security/

Institutional landscape

European External Action Service (EEAS)

The EEAS handles cybersecurity cooperation between the EU and external countries and organizations, guided by the EU Cybersecurity Strategy. EEAS is especially important for cyber defence management.[129]

The European Commission Directorate General for Communications Networks, Content & Technology (DG CONNECT)

DG Connect is the main Directorat General for managing issues of cybersecurity.[130]

DG Home

Responsible for cybercrime prevention and management.[131]

European Agency for Network and Information Security (ENISA)

ENISA is the main EU agency for cybersecurity management. ENISA has been continuously strengthened and gained increasing responsibility since its set up in 2004, and plays an important role in the coming implementation of the NIS-directive and the facilitation of the thereby established cybersecurity networks. ENISAs core tasks surrounds recommendations, support of both the EU institutions as well as Member States with cybersecurity policy making and implementation of cybersecurity policy, promoting a culture of Network and Information Security within the Union and raise awareness of its importance. ENISA works both operationally and hands on with, for example workshops and conduction of cybersecurity exercises, as well as academically with publications and studies on, for example, Secure Cloud Adoption, cyber crisis management, identification of best practises, privacy issues and issues critical information infrastructure as well as the cyber threat landscape.[132]

Europan Cybercrime Centre (EC3)

The EC3 started 2013 with the objective to improve the capacity of the EU to respond to cybercrimes against businesses, individuals and governments. This was based on the notion that the EU has become increasingly vulnerable to cybercrimes due to the ever more advanced and extensively used internet infrastructure, combined with economies and payment systems depending on the internet. EC3

[129] EU Cyber Defence Policy Framework, as adopted by the Councilon 18 November 2014, p. 6
[130] https://ec.europa.eu/digital-single-market/dg-connect
[131] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/organized-crime-and-human-trafficking/cybercrime/index_en.htm
[132] https://www.enisa.europa.eu/about-enisa

is situated under EUROPOL, and have three main focus areas; 1. Organised cybercrime, for example online fraud. 2. Cybercrimes with serious harmful implications to victims, and 3. Cybercrimes which affects CIP or CIIP (including cyberattacks). The EC3 has several functions, ranging from coordination of cybercrime combating actors to operational support of Member State cybercrime operations and conducting training of Member State authorities.[133]

CERT-EU

CERT-EU is the Computer Emergency Response Team of the EU institutions and agencies. CERT-EUs mission is to support EU institutions through providing services ranging from prevention and detection to response and recovery. Among its main tasks are; early warning and alerts, information on cyberattacks and vulnerabilities, as well as coordination of incident response. [134]

Joint Research Centre

"The JRC is supporting the EU Critical Information Infrastructure Protection (CIIP) Action Plan by contributing to the organisation of pan-European cyber-security exercises. The JRC is also researching technical solutions to increase the level of realism of these exercises and is developing technical guidelines to help the preparation and implementation of cyber exercises in a multinational context."[135]

Sub-sectors within this area

Critical Information Infrastructure Protection (CIIP)

Critical Information Infrastructure Protection, Cyber Security and Critical Infrastructure Protection are sectors/areas of protection which are very entangled, even if they should not be mistaken as the same. ENISA defines (based on the Council Directive 2008/114/EC on the identification and designation of European Critical Infrastructures) Critical Information Infrastructures as *"ICT (cyber) systems that are Critical Infrastructures for themselves or that are essential for the operation of Critical Infrastructures (telecommunications, computers/software, Internet, satellites, etc."*[136] Examples of CII are *Industrial Control Systems* (ICS) which supports industrial processes, for example SCADA (Supervisory Control and Data Acquisition) systems. With increased efficiency of these networks through interconnection, the vulnerability of these networks has increased as well.[137] Another example is the use of *Smart Grids*, "smart" electricity networks with the possibility of integrating behavior and action of users in order to create secure and efficient energy supply. Just like with SCADA systems

[133] https://www.europol.europa.eu/ec3
[134] RFC 2350, ERT-EU p. 2013, p.1
[135] https://ec.europa.eu/jrc/en/research-topic/cybersecurity
[136] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/cii
[137] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada

however, the efficiency comes with the price of vulnerability.[138] Critical Infrastructure on the other hand, also by the definition by the Directive 2008/114/EC is defined like this; *"an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;".*[139] Thus, Critical Infrastructure Protection does not have to involve Critical Information Infrastructure Protection, even if it often does. Cyber security, or Network and Information Security, in turn, entails more than CIP or CIIP. This could be highlighted by the strategic priorities of the EU Cybersecurity Strategy;

- Achieving cyber resilience
- Drastically reducing cybercrime
- Developing cyberdefence policy and capabilities related to the Common Security and Defence Policy (CSDP)
- Develop the industrial and technological resources for cybersecurity
- Establish a coherent international cyberspace policy for the European Union and promote core EU values

Cyber security and critical information infrastructure becomes an important aspect of CIP since essential services (including energy, transport and satellite systems) rely on cyber for its services, thus becoming vulnerable to cyber threats which may hinder;

- "Confidentiality – unauthorized access to or interception of information." [140]
- "Integrity – unauthorized modification of information, software, physical assets." [141]
- "Availability – blockage of data transmission and/or making systems unavailable." [142]

"Recent deliberate disruptions of critical automation systems prove that cyber-attacks have a significant impact on critical infrastructures and services. Disruption of these ICT capabilities may have disastrous consequences for the EU Member States' governments and social wellbeing. The need to ensure ICT robustness against cyber-attacks is thus a key challenge at national and pan-European level. Today ICS products are mostly based on standard embedded systems platforms and they often

[138] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/scada
[139] Directive 2008/114/EC, p.3
[140] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf
[141] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf
[142] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf

use commercial off-the-shelf software. This results in the reduction of costs and improved ease of use but at the same time increases the exposure to computer network-based attacks."[143]

Based on this, critical infrastructure-sectors have started to develop cyber security measures, both on policy level as well as technical level. For example, the **Energy Expert Cyber Security Platform Expert Group** and **The Galileo PRS.**

European Public-private Partnership for Resilience (EP3R)

The EP3R was established in 2009 in order to engage the EU-level with National Private Public Partnerships to address Critical Information Infrastructure Protection (CIIP) issues at European level. One of the reasons for the establishment of the EP3R was an analysis by ENISA in 2010, which identified barriers for information sharing in the field of Critical Information Infrastructure Protection (CIIP). [144]

According to the study the most important barriers were:

- Economic incentives stemming from cost savings;
- Incentives stemming from the quality, value, and use of information shared;
- As most important barriers were identified:
- Poor quality of information;
- Misaligned economic incentives stemming from reputational risks;
- Poor management. [145]

The study revealed that the critical information infrastructures (CII) sector was fragmented both geographically and due to the competition among telecom operators. Increasing the Resilience of those CIIs was generally seen as fundamental within Member States and several National Public-Private Partnerships (PPPs) were already established to enhance preparedness and response to disasters or failures by coordinating the efforts among telecom operators. Cross-border mechanism were set up on an ad hoc basis, but there was a need for global approach at a European level arose to respond to both existing and emerging threats.

"In March 2009, the European Commission adopted a policy initiative - COM (2009)149 - on Critical Information Infrastructure Protection (CIIP) to address this challenge and a European Public-private Partnership for Resilience (EP3R) was established in order to support such coordination." [146]

[143] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services

[144] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[145] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r

[146] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

The objectives of the EP3R was to discuss policy priorities, baseline requirements, enhance information sharing and to promote adoption on best practises for security and resilience. ENISA was the facilitator of the Ep3R. [147] The Ep3R closed during 2013.

Cyber Defence

Developing an EU Cyberdefence Framework was included as one of the measures of the EU Cybersecurity Strategy 2013. Hence, the EU Cyber Defence Policy Framework was adopted by the Council in November 2014. It outlines priorities for the EU cyber defence and defines roles and responsibilities. Included in the priorities are;

- Development of Member State cyber defence capabilities in order to ensure networks supporting the CSDP.[148] This involves improving cooperation and coordination between Member States on monitoring, situational awareness, prevention, detection and protection, information sharing, forensics and malware analysis capability, lessons learned, damage containment, dynamic recovery capabilities.[149] It also involves increased cooperation between military CERTs and support of development of pooling and sharing regarding cyber defence operations. [150] Member States might ask ENISA for advice and assistance when cyber defence capabilities depends on civilian cyber security. [151] Moreover, increased information sharing on, for example, training, exercises and programmes. [152]
- The EEAS aims to develop its own cyber security capacity (even if CERT-EU still is the central cyber incident response team for EU bodies). In lead of this work is the EEAS MDR (Managing Directorate for Resources) supported by the European Union Military Staff (EUMS), Crisis Management and Planning Directorate (CMPD) and Civilian Planning and Conduct Capability (CPCC). [153]
- Promote Civil-Military cooperation on cybersecurity, including joint exercises, information exchange, risk assessments and early warning mechanisms.[154]
- Increase cyber defence research and technology. [155]
- Improve training and exercise activities. [156]
- Enhancement of cooperation with international partners.

[147] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ppps/public-private-partnership/european-public-private-partnership-for-resilience-ep3r
[148] EU Cyber Defence Policy Framework, 2014, p. 3
[149] EU Cyber Defence Policy Framework, 2014, p. 5
[150] EU Cyber Defence Policy Framework, 2014, p. 5
[151] EU Cyber Defence Policy Framework, 2014, p. 5
[152] EU Cyber Defence Policy Framework, 2014, p. 5
[153] EU Cyber Defence Policy Framework, 2014, p. 6
[154] EU Cyber Defence Policy Framework, 2014, p. 6
[155] EU Cyber Defence Policy Framework, 2014, p. 6
[156] EU Cyber Defence Policy Framework, 2014, p. 6

Moreover, the framework states that “the objectives of cyberdefence should be better integrated within the EU’s crisis management mechanisms.”[157]

Inventory

Detection

*The CSIRT Network

CSIRT stands for Computer Security Incident Response Team. Another common acronym referring to the same type of team is CERT (Computer Emergency Reponse Team). CSIRTs/CERTs can be found at various levels and sectors of societies. However, a national CSIRT is a team responsible for the national response to (and prevention of) cybersecurity incidents and risks. They are key players when it comes to detection, early warning and rapid alert of cyber incidents and crises. Before the NIS-directive, the connections between national CSIRTs in the EU were quite informal. However, the NIS-directive has several measures regarding CSIRTs. First, Member States are required to establish National CSIRTs if they have not already done it. Secondly, the Directive establishes a formal EU network of national CSIRT’s, called the CSIRT Network, in coordination of ENISA. [158]

According to the NIS-directive, operators of critical services must report cyber incidents to their national CSIRT or to their national authority handling cybersecurity – if they are severe enough to have significant impact on the continuity of the service in question. The information about the incident must be thorough enough for the CSIRT/authority to make an assessment of the possible cross border effect of the incident. However, the incident reporting is not supposed to expose the reporting actor but preserve confidentiality of the information (which is important since information about breaches might be very sensitive and can affect both commercial interests as well as security of the affected actor).[159]

The CSIRT or authority is required to let the Member States who has essential services which might be significantly affected by the incident get information about it through the CSIRT-network.[160]

*European Cybercrime Centre (EC3)

Among the EC3’s main objectives are improving the overall EU as well as Member State individual preventive capabilities when it comes to cybercrime. In order to achieve this, EC3 conducts vulnerability scannings and distribute early warnings on cyber risks and threats. [161]

[157] EU Cyber Defence Policy Framework, 2014, p. 3
[158] https://www.enisa.europa.eu/topics/national-csirt-network/capacity-building
[159] The NIS-directive Brussels, 18 December 2015, 15229/2/15 REV 2, p. 39-40
[160] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 43
[161] https://www.europol.europa.eu/ec3

Sensemaking

*The CSIRT Network

The CSIRT network will have sense-making tasks such as;

- "At the request of the representative of a Member State potentially affected by an incident, exchange and discuss non-commercially sensitive information related to that incident and associated risks. (Any Member State may refuse to contribute to that discussion if there is a risk of prejudice to the investigation of the incident)". [162]
- "Exchange and make available on a voluntary basis non-confidential information on individual incidents".[163]

*The Cooperation Group

With the implementation of the NIS-directive (expected in August 2016), The Cooperation Group is to be established. It will be composed of representatives from Member States respective CSIRT, as well as CERT-EU (the CSIRT of EU institutions) and ENISA. The Commission will also have representatives in the group and provides the secretariat. When assessed appropriate, the group can let other stakeholders join its work. To build capacity and knowledge among Member States, the cooperation group should, according to the NIS directive, also serve as an instrument for the exchange of best practices, discussion of capabilities and preparedness of the Member States and on a voluntary basis assisting its members in evaluating national NIS strategies, building capacity and NIS exercises.[164]

The Cooperation Groups main focus and its tasks will be mostly preventive. Among the Cooperation Groups tasks are to;

- "Provide strategic guidance for the activities of the CSIRTs network established under Article 8b of the NIS-directive." [165]
- "Exchange best practice on the exchange of information related to incident notification referred to in Article 14(2ac) and 15a(2) of the NIS-directive." [166]
- "Exchange best practices between Member States and, in collaboration with ENISA, assist Member States in building capacity in NIS." [167]

[162] The NIS-directive, Brussels, 18 December 2015, 15229/2/15 REV 2 p. 36
[163] The NIS-directive, Brussels, 18 December 2015, 15229/2/15 REV 2 p. 36
[164] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 6
[165] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[166] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[167] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35

- “Discuss capabilities and preparedness of the Member States, and, on a voluntary basis, evaluate national NIS strategies and the effectiveness of CSIRTs, and identify best practices.” [168]
- “Exchange information and best practice on awareness raising and training.” [169]
- “Exchange information and best practice on research and development on network and information security.” [170]
- “Discuss, with representatives from the relevant European Standardisation Organisations, the standards referred to in Article 16 of the NIS-directive.” [171]

*The European Cybercrime Centre (EC3)

Besides early warnings, the EC3 also performs cyber threat assessments. [172]

Among the EC3 tasks are;

- Awareness raising initiatives on cybercrimes and online threats.
- Suggesting preventive measures to legislators. [173]
- “Being the central hub for criminal information and intelligence.” [174]
- “Providing a variety of strategic analysis products enabling informed decision making at tactical and strategic level concerning the combating and prevention of cybercrime;”[175]
- “Providing highly specialised technical and digital forensic support capabilities to investigations and operations.”[176]

European Cybercrime Training and Education Group (ECTEG)

Regarding training, the EC3 works closely to the European Cybercrime Training and Education Group(ECTEG). ECTEG consists of Member States law enforcement agencies as well as other relevant actors from the private sector, academia and even international actors. [177] Among the aims of the ECTEG are; - information sharing between various actors, harmonise training and finding common solutions to identified issues. [178]

[168] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[169] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[170] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[171] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[172] https://www.europol.europa.eu/ec3
[173] https://www.europol.europa.eu/ec3/public-awareness-and-prevention
[174] https://www.europol.europa.eu/ec3/
[175] https://www.europol.europa.eu/ec3/
[176] https://www.europol.europa.eu/ec3/
[177] http://www.ecteg.eu/
[178] http://www.ecteg.eu/

*ENISA

ENISA, the European Agency for Network and Information Security, is mainly focused on preparation. This is highlighted by the stated priorities of ENISA's work;

- "To anticipate and support Europe in facing emerging network and information security challenges, by collating, analyzing and making available information and expertise on key NIS issues potentially impacting the EU, taking into account the evolutions of the digital environment."[179]
- "To promote network and information security as an EU policy priority, by assisting the European Union institutions and Member States in developing and implementing EU policies and law related to NIS." [180]
- "To support Europe maintaining state-of-the-art network and information security capacities, by assisting the Member States and European Union bodies in reinforcing their NIS capacities." [181]

ENISA has a wide range of preparation activities, and is a key player for the implementation of the NIS-Directive. Among the preparation activities of ENISA are;

- Building capacity of national CSIRTs through, for example, guidance on how to facilitate a CSIRT, training and exercising for CSIRTs. [182]
- **The Cyber Exercise Platform** is a new initiative from ENISA, which aims to promote information sharing on cybersecurity exercises practises and lessons learned, as a step of building a cyber security exercise community. It provides a platform where actors can publish information about their exercises and get access to information about others.[183]
- Papers and studies on, for example, Cloud Security, Cyber Crisis Management, Critical Information Infrastructure Protection, Cyber risks and The Cyber Threat Landscape.
- Promotes awareness raising of cyber threats, through initiatives such as **the European Cyber Security Month** each year in October.[184]
- Provides expertise, advice and recommendations to Member States on cybersecurity issues, both preventive and reactive.[185]
- Conducts workshops and training courses for Cyber Security Specialists.[186]

[179] https://www.enisa.europa.eu/about-enisa/mission-and-objectives
[180] https://www.enisa.europa.eu/about-enisa/mission-and-objectives
[181] https://www.enisa.europa.eu/about-enisa/mission-and-objectives
[182] https://www.enisa.europa.eu/topics/national-csirt-network/csirt-capabilities
[183] https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform
[184] https://www.enisa.europa.eu/topics
[185] https://www.enisa.europa.eu/about-enisa
[186] https://www.enisa.europa.eu/topics

*The NIS-Platform (working groups)

In order to foster resilience of networks, and help implement the measures set out in the cybersecurity strategy of the EU and the NIS-directive, and harmonize its application, the NIS Public-Private Platform was established in 2013. The NIS-platform consists of three working groups focusing on (amongst other things) risk management and awareness raising, information exchange, risk metrics, incident coordination. The three working groups are;

The NIS-platform aims to be cross-cutting, involving various relevant sectors and both private and public actors, and therefore be able to identify cross cutting and horizontal best practises.[187]

*CERT-EU

CERT-EU is primarily focused on supporting EU institutions with detection and alerts but also works together with Member State national CSIRTs (and now the CSIRT-network) regarding incident preparation through, for example, exchange of good practices. [188]

The Joint Research Centre's Experimental Platform for ICT (information and communication technology) Contingencies (EPIC)

The Experimental Platform for Internet Contingencies (EPIC) is a platform which can simulate the impact of various cyberattacks and disruptions. The platform may be used for cybersecurity experiments and exercises.[189]

The Joint Research Centre's Classification System for Critical Infrastructure Protection with focus on Cyber Security

The JRC is currently building a classification system which will result in a measurement system for measuring the severity of cyber incidents as well as a taximony focusing on cyber security, which will improve information exchange on cybersecurity issues as well as common assessments on the severity of cybersecurity incidents.[190]

The Public-Private Partnership (PPP) on cybersecurity (2016)

The Commission will establish a new EU Public-Private Partnership on Cybersecurity during 2016. Although it is still unclear exactly what tasks this PPP will perform, it aims to align and build trust amongst member states and industrial actors and thereby boost cybersecurity alignment and cooperation. [191]

[187] https://resilience.enisa.europa.eu/nis-platform
[188] RFC 2350, ERT-EU p. 2013, p.1
[189] https://ec.europa.eu/jrc/en/research-topic/cybersecurity
[190] https://ec.europa.eu/jrc/en/research-topic/cybersecurity
[191] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing

Decision Making

The EU Standard Operational Procedures to manage multinational cyber-crises

The EU-SOPs, developed by the EU and European Free Trade Association (EFTA) Member States in collaboration with ENISA, guides the handling of major cyber incidents that could possibly escalate to a cyber crisis. The aim of the SOP includes;

- "Increasing the understanding of the causes and impact of multinational cyber crises (situational awareness) and allow for quick and effective mitigation. Through a combination of contact points, guidelines, workflows, templates, tools, and good practices, the EU-SOPs offer European crisis managers the ability to use the internationally shared technical and non-technical information to draw an integrated operational picture and identify effective action plans. These can be presented to the political level for decision making." [192]
- ENISA assists the European Commission whenever required, in order to achieve a coordinated response to cyber incidents or crises. The main framework mentioned for this is the Integrated Political Crisis Response arrangements.[193]

Coordination

*The European Cybercrime Centre (EC3)

The EC3 aims to be an information hub and enhance coordination of actors in both preventing and responding to threats. This includes supporting Member States' operations and investigations by means of coordination and expertise, as well as connecting of law-enforcement actors with non-law enforcement actors for enhanced cooperation.[194] The EC3 aims to be able to have an overview of cybercrime battling capacities throughout the EU, which makes it possible for the EC3 to target where assistance is needed and avoid overlaps. Moreover, one of the tasks of the EC3 it to be a focal point, bringing relevant experts and actors together from both the EU and from outside the EU, and strengthen partnerships on cybercrime. The so called "Outreach function" allows EC3 to proactively engage with new partners and build cooperation with various stakeholders important for battling cybercrime, such as EU institutions, the private sector, academia, law enforcement agencies and international organizations. [195]

[192] https://www.enisa.europa.eu/news/enisa-news/standard-operational-procedures-to-manage-multinational-cyber-crises-finalised-by-eu-efta-member-states-and-enisa
[193] https://www.enisa.europa.eu/topics/cyber-crisis-management/eu-cooperation
[194] https://www.europol.europa.eu/ec3/
[195] https://www.europol.europa.eu/ec3

*The CSIRT Network

One of the objectives of the NIS-directive is to enhance CSIRT operational cooperation, including incident management. Besides building trust and enhance preparedness which will improve the overall response capability of Member States, The CSIRT network will have some specific tasks relating coordination, and shall;

- "At the request of the representative of a Member State's CSIRT, discuss and, where possible, identify a coordinated response to an incident that has been identified within the jurisdiction of that same Member State." [196]
- "Support Member States in adressing cross-border incidents on the basis of their voluntary mutual assistance."[197]

*ENISA

In cooperation with EC3, ENISA facilitates the coordination between relevant authorities and law enforcement agencies. ENISA also aims to enhance coordination between member states, EU bodies and NIS stakeholders (private sector), by reinforcing cooperation between them. [198]

The NIS-Platform (working group 2)

In order to foster resilience of networks, and help implement the measures set out in the cybersecurity strategy of the EU and the NIS-directive, and harmonize its application, the NIS Public-Private Platform was established in 2013. It consists of several working groups. WG2 focuses on information exchange and incident coordination, incident reporting and risk metrics regarding information exchange.

Meaning Making/ Communication

ENISA cyber incident website

As a crisis communication measure, the CSIRT-networks secretariat (ENISA) is also encouraged (by the NIS-directive) to setup a website where information sharing about major cyber incidents or crises might be published. This is based on the notion that the EU-level should be able to provide such a service since both businesses and individuals operates more and more online, outside of national borders. The NIS-Directive furthermore encourages the members of the CSIRT-network to, voluntarily, share non sensitive information about incidents on this website. [199]

[196] The NIS-directive, p. 36

[197] The NIS-directive, p. 36

[198] https://www.enisa.europa.eu/about-enisa/mission-and-objectives

[199] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 7

The Galileo Public Regulated Service

The PRS is a service which ensures continuity, more specifically service to authorized users when access is denied to other navigation services. It will provide a protected signal for critical application. The PRS can be useful for EU public safety and emergency services. [200]

Good Practise Guide on Information Sharing

Based on the need for public private cooperation on the EU-level regarding cybersecurity and CIIP, ENISA collected experiences form existing PPPs which resulted in the **Good Practise Guide on Information Sharing,** which aims to assist Member State to establish information exchange between Private and Public actors. [201]

Accountability

*The CSIRT Network lessons learned

Regarding recovery, the CSIRT-network shall, according to the NIS-directive;

- "Discuss lessons learned from NIS exercises, including from those organised by ENISA. i. At the request of an individual CSIRT, discuss the capabilities and preparedness of that same CSIRT." [202]
- "As input to the Commission's periodic review of the functioning of the Directive, the CSIRTs network shall every one and a half years produce a report assessing the experience gained with the operational cooperation, including conclusions and recommendations, pursued under article 4. That report shall also be submitted to the cooperation group."[203]

CERT-EU's activities cover recovery, however from a quite technical perspective and focused on the EU institutions only.[204]

*The Cooperation Group lessons learned

The Cooperation Group shall, according to the NIS-directive;

- "Where relevant, exchange experiences on matters concerning NIS with relevant Union institutions bodies, offices and agencies." [205]
- "Collect best practice information on risks and incidents affecting network and information systems'"[206]

[200] http://www.gsa.europa.eu/security/prs
[201] https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
[202] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 36
[203] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 37
[204] RFC 2350, ERT-EU p. 2013, p.1
[205] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[206] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35

- “Examine on an annual basis the summary reports referred to in Article 6(4ab new).” [207]
- “Discuss the work undertaken with regard to NIS exercises, education programmes and training, including the work by ENISA. “[208]

*Cyber Europe after action reports

After action published at ENISAs website - providing overviews over the main problems, prospects and successes identified when performing the respective exercises, including lessons learned. The Cyber Europe 2014 after action report also included an action plan.[209]

The Cyber Exercise Platform, which is currently in the build-up stage, will provide opportunities to share and search for lessons learned from cybersecurity exercises. The Platform will provide actors with the possibility of reporting their cyber exercises, including objectives, type of exercise, and lessons learned. Starting with some 200 cyber exercises and with actors continuously adding conducted exercises to the database, the objective with the platform is that it will become a source of lessons learned from a great variety of cyber incident scenarios, and create the possibility for actors to learn from others successes and mistakes regarding cyber incident management. [210]

[207] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[208] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 35
[209] https://www.enisa.europa.eu/publications/ce2014-after-action-report
[210] The 2015 Report on National and International Cyber Security Exercises, p.9

The Energy Sector

Introduction

General background

The EU energy sector is complex and entails complex risks and security issues. The risks of disruption depends on a number of variables combined, such as suppliers, transport, supply points (such as infrastructure, ports and pipelines), political stability in countries, fuel routes etc. Since the energy sector is highly transboundary, EU member states are not only dependent on energy, but they are also highly interdependent and connected. Energy security involves many different aspects, including enhancement of security of supply by decreasing dependence of energy import, protection of disruption caused by, for example, cyberattacks affecting the energy grid, individual Member State national measures to ensure continuity and enhanced energy security. One of the security-problems of the energy sector is that efficiency increases vulnerability. For example, when effectivity increases with the use of "Smart Grids" and interconnected Energy Grids, vulnerability increases as well. Smart Grids improves control over electricity consumption and distribution to the benefit of consumers, electricity suppliers and grid operators. However, it comes with the cost of exposure of the network for directed cyberattacks against power generation plants.[211] Possibly the most famous and sophisticated cyberattack to this date was the malware called "STUXNET", discovered in 2010, which successfully disrupted the uranium enrichment infrastructure in Iran by causing its centrifuges to spin themselves apart.

The threat is also exemplified in the Commission Staff Working Document on the new approach to EPCIP, which also points out Energy as one of the main Critical Infrastructure sectors;

- "As the wide-area black-outs of past years have shown, a single incident affecting one significant element of the grid can affect supply on the whole continent. Threats (man-made) also have similar aims and modus operandi across country borders, while single attackers or coordinated action may target networks on a regional, European or international scale, as is the case with cyber-attacks." [212]

The SWD continues to state that;

- "This calls for a coordinated protection mechanism, involving all operators and their sectoral bodies. The risks associated with the above threats can only be properly tackled by response at system level, as the integrity and functionality of the whole system is affected. The sector (ENTSO-E in particular) has already invested in CIP measures and has expressed strong support for an EU approach that would also tie in with the requirements of the internal market

[211] https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services

[212] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. P.14

regulations."[213]

An increase of integration of the EU energy system (in combination with the fact that Member State import energy from the same countries) also enhances vulnerability. [214]

The EU's overall crisis management work and measures for CIP (including frameworks, key documents, exercises and networks) are related to and entangled in the crisis management work and measures of the energy sector.

The EU has long been involved with preparing for and enhancing energy security, given the crucial part of energy to the daily lives of EU citizens. Indeed, much has been done in the "Preparation" department, considering that "Energy" is largely entailed in the EU efforts to enhance Critical Infrastructure Protection and Critical Information Infrastructure Protection.

Increasing trade and interconnectedness in electricity between Member States has resulted in that short time surpluses of one form of electricity in one Member State can flow to counter deficits in another. [215] Moreover, the ongoing work of building up flexibility in Europe's gas and electricity infrastructure has enabled a more efficient use of reserves. [216] Since the 2006 and 2009 gas supply crises, the EU has strengthened its coordination capabilities in order to prevent and mitigate possible gas supply disruptions. There are European rules to secure supplies to protected customers (e.g. customers that use gas for heating) in severe conditions, including in the case of infrastructure disruption under normal winter conditions, and Member States need to draw up Emergency Preparedness Plans and Emergency Response Plans. The Gas Coordination Group, involving Member States, regulators and all stakeholders, has proven to be an effective EU-wide platform to exchange information between experts and coordinate action. These rules provide a European framework that creates trust and ensures solidarity as it guarantees that Member States act on their national responsibilities and collectively enhance security of supply.

[213] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. P.14

[214] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 4-5

[215] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 16

[216] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 16

Policy Background

Critical Infrastructure Protection: Energy

Since the energy-sector is one of the main sectors in the CIP-efforts of the EU, the policy background of CIP is highly relevant for energy.

- During 2004, The Council asked for an overall strategy of CIP.[217]
- During October 2004 the Commission adopted the "**Communication on Critical Infrastructure Protection in the Fight against Terrorism**". [218]
- Deriving from the Council conclusions on "**Prevention, Preparedness and Response to Terrorist Attacks"** and the **"EU Solidarity Programme on the Consequences of Terrorist Threats and Attacks"**, the Commission proposed the **European Programme for Critical Infrastructure Protection (EPCIP)** and agreed to the setting up by the Commission of a **Critical Infrastructure Warning Information Network (CIWIN)** [219]
- In 2008, the **Directive on European Critical Infrastructures** introduced a common approach on how to improve CIP in the EU and suggested a procedure for identification of critical infrastructures. It was only focused on energy and transport sectors, and required operators in these sectors to prepare continuity plans and linking them to national authorities involved in CIP.[220]
- In 2009, the **Communication on Critical Information Infrastructure protection (CIIP)** was published. [221]
- In 2011, the Commission evaluated the CIP achievements and published follow-up actions in on **"Achievements and next steps: towards global cyber-security"**, stating again the importance of a common EU approach to CIP.[222]
- In 2012, there was a review of EPCIP, revealing capability gaps in cross-sectorial CIP issues. This led to the **"2013 Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection"**. One of the highlighted measures of this document is continuous focus on discovering crisis management and CIP tools and

[217] Brussels, 12.12.2006, COM(2006) 786 final COMMUNICATION FROM THE COMMISSION, p. 1
[218] Brussels, 12.12.2006, COM(2006) 786 final COMMUNICATION FROM THE COMMISSION, p. 1
[219] Brussels, 12.12.2006, COM(2006) 786 final COMMUNICATION FROM THE COMMISSION, p. 1
[220] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm
[221] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip
[222] https://ec.europa.eu/digital-single-market/en/news/policy-critical-information-infrastructure-protection-ciip

processes with **“The Four”** chosen Cis of the EU dimension, two of them related to the Energy-sector (**The Electricity Transmission Grid** and **The Gas Transmission Network**)

Sector	Subsector(s)	Description
Energy	**Electricity**	**Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity**
Energy	**Oil**	**Oil production, refining, treatment, storage and transmission by pipelines**
Energy	**Gas**	**Gas production, refining, treatment, storage and transmission by pipelines** **LNG terminals**

Table: Description of the energy-sector in the **Communication on Critical Information Infrastructure protection (CIIP).**

- In 2013, the **Cybersecurity Strategy of the EU** and **The NIS-directive proposal** was published, suggesting that companies and actors within critical infrastructure sectors (including energy) will be required to;
- Report to the cybersecurity authorities (or CSIRT) cyber incidents that may significantly affect the continuity of critical services .[223]
- Assess and manage cyber risks.[224]

The expected implementation of the NIS-directive is August 2016, which will make these requirements legally binding for Member States. [225]

[223] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

[224] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

[225] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

Energy

- Regulation 994/2010 is vital to security of supply (rather the absence of potential security disruption) for example, common indicators (labelled the N-1 standard) to measure threats to gas security for example to gas installations on national level but also their operational status. It also regulates what member states with a gas system must do;

- Perform Risk analysis (RA),
- Develop preventive action and emergency plans (PAPs and EPs respectively). This is a sequential process beginning with the RA, outlining risks and hazards that the PAPs and EPs must then address depending on the situation. The PAP is intended to assemble any market-based measures available that may be utilised to avoid, or at least mitigate impact, of risks identified in the RA – as such the PAPs are relevant in a pre-crisis situation and thus a prevention capacity

- During 2014, the 2009 Nuclear Safety Directive was amended to reinforce existing obligations and to introduce new ones, including requirements of Member States to carry out safety assessments of new power plants and ensuring safety enhancement of old reactors. [226]

- In 2014, the Commission adopted the Communication on a **''European Energy Security Strategy" (EESS)** and the related **Staff Working Document**. The EESS is a result of the identified need for a comprehensive approach to energy security within the EU, as well as a result of the happenings at the EUs eastern borders, which provoked questions about the EU capability to cope with energy supply disruptions both short and medium term. The strategy is focused around 8 objectives;[227]

1. Immediate actions aimed at increasing the EU's capacity to overcome a major disruption during the winter 2014/2015;
2. Strengthening emergency/solidarity mechanisms including coordination of risk assessments and contingency plans; and protecting strategic infrastructure;
3. Moderating energy demand;
4. Building a well-functioning and fully integrated internal market;
5. Increasing energy production in the European Union;
6. Further developing energy technologies;
7. Diversifying external supplies and related infrastructure;

[226] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 7

[227] COMMISSION STAFF WORKING DOCUMENT on the European Energy Security Strategy, 2015, p.2

8. Improving coordination of national energy policies and speaking with one voice in external energy policy.[228]

The key actions described in the strategy are;

- "Intensified cooperation with the Gas Coordination Group and notably continue monitoring natural gas flows and the level of gas storage and coordinate at EU and/or regional level national risk assessments and contingency plans."
- "Update the risk assessments and the Preventive Action Plans and Emergency Plans, as provided for by Regulation 994/2010"
- "Launch energy security stress tests in light of the supply disruption risks in the upcoming winter, and develop back-up mechanisms if necessary; such as increasing gas stocks, developing emergency infrastructures and reverse flows and reducing energy demand or switching to alternative fuels in the very short term"
- "Further cooperate with gas suppliers and transmission system operators to identify possible sources for short-term additional supplies, notably LNG."
- " Strengthening emergency/solidarity mechanisms including coordination of risk assessments and contingency plans; and protecting strategic infrastructure"

The strategy also states that;

- Member States are obliged to build up and maintain minimum reserves of crude oil and petroleum products and this will mitigate the risks of supply disruption.
- Member States are obliged to invest in back-up infrastructure.
- "The solidarity that is the hallmark of the EU requires practical assistance for those Member States most vulnerable to severe energy supply disruptions. Proper contingency planning, based on stress tests of the energy systems and discussions with national authorities and industry, should therefore be organized and regularly reviewed, with the aim of guaranteeing minimum levels of intra-EU deliveries of alternative fuel supplies to complement emergency stocks. In view of current events, the immediate focus should be on Member States on the eastern border of the EU; where appropriate, candidate countries and potential candidates could be associated to such mechanisms". [229]

- In early 2015, the "**Energy Union Framework Strategy"** was adopted. The EESS was included as a part of the EUFS, stating that energy security is one of the five mutually dependent and interlinked dimensions of the Energy Union.[230]

[228] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0330&qid=1407855611566

[229] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52014DC0330&qid=1407855611566

[230] COMMISSION STAFF WORKING DOCUMENT on the European Energy Security Strategy, 2015, p.2

Earlier energy crises in the EU

The German transmission grid 2006

“An extensive power disruption occurred in the north German transmission grid on 4 November 2006, and was felt over most of the continent, including Austria, Belgium, France, Slovenia and Spain, in addition to Germany. Although the action taken by the transmission system operators (TSOs) prevented the blackout, this case is considered among the most severe and largest disturbances ever in Europe. The effects were important in terms of power cuts at industrial and domestic level (more than 15 million households), while electricitydependent services such as transport were affected (for example hundreds of trains were cancelled or delayed).” [231]

Brotherhood Pipeline 2009

“The physical threats (ranging from terrorism to boycotts and strikes), disruptive natural events (earthquakes, floods, very cold periods, big storms) and commercial disputes to which the gas network is subject make it vulnerable and jeopardises Europe’s secure access to gas. An illustrative example of the effects of a disruption of the gas network is the Brotherhood pipeline case of 2009. This pipeline, which transports almost 300 million cubic metres of Russian gas every day to Europe, passing through Ukraine, started reducing its flow in early January, leading to a complete shutdown. Its disruption had a significant impact on many Member States, in particular those that depend exclusively on this supply route, leaving homes without gas for heating and forcing production stops in some industries. Gas supplies were only fully restored on 21 January 2009. This disruption was the most serious of its kind in Europe in recent history: for an unprecedented period of two weeks, Europe was cut off from 30% of its total gas imports, an equivalent of 20% of its gas supplies.”[232]

Russian-Ukrainian-EU Gas Dispute 2014-2015

In relation to the Crimea crisis, Moscow threatened to cut gas supply to Ukraine, thus causing disruption to the rest of the EU as well. Even if the dispute was solved, the possibility of supply disruption sparked the EU efforts to enhance energy security and its capability to manage short and medium term supply disruption.[233]

[231] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. P.14
[232] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure. P.15
[233] http://www.nato.int/docu/review/2014/NATO-Energy-security-running-on-empty/Ukrainian-conflict-Russia-annexation-of-Crimea/EN/index.htm

Institutional landscape

- **Commission:** Miguel Arias Cañete (2014-2019), Climate Action and Energy.
- **DG**: DG ENER
  - 5 subdirectorates: A – Energy Policy, B – Internal Energy Market, C – Renewables etc., D – Nuclear energy etc., E – EURATOM safeguards & SRD (shared resource directorate ENER & MOVE)

Upon the allocation of portfolios to Commissioners in 2010 a disassembly of DG TREN took place, leading to the creation of the DG's MOVE and ENER. Along with the departments within TREN dealing with energy issues the Task Force Energy from the External Relations DG was transferred to ENER. The work carried out within DG ENER has since been streamlined with the Europe 2020 economic strategy presented by the Commission in 2010 and reformulated into the DG specific Energy 2020 strategy. As such, the main task of ENER according to its mission statement is to develop and implement the EU energy policy in three different areas: the **energy market, promote sustainable energy production** and enhance conditions for **safe and secure supply**. Out of the three the most relevant area from a crisis management perspective is safe and secure supply. The area of safe and secure supply is linked to the energy market and sustainability issues, as can be seen below and thus it is not as clearly cordoned off as one might expect.

- **Leadership**:
  - Dominique Ristori (director-general)
  - Christopher Jones (Deputy Director-general A,B,C)
  - Gerassimos Thomas (Deputy Director-General D,E).
  - Mechthild Wörsdörfer (A)
  - Klaus-Dieter Borchardt (B)
  - Marie Donnelly (C)
  - Massimo Garribba (D)
  - Piotr Szymanski (E)
  - Agnieszka Kazmierczak (SRD).

Agencies: EURATOM (and ESA), ACER (INEA, EASME), ENISA (cybersecurity in relation to critical infrastructure protection), JRC.

Sector relevant outside DG: Project Team Energy Union led by Maroš Šefčovič and Miguel Arias Cañete who has been tasked by Commission President Juncker to "strengthen energy security on a European Scale" with reference to security of supply.

Sub-sectors within this area

Oil

- Oil is the primary energy source used in the EU, mainly fueling the transport sector (64% of the consumption). The EU is highly dependent on import, which is about 80% of the consumption – making the EU quite vulnerable for price changes. [234] In order to cope with temporary disruptions, the EU has created emergency oil stocks. Demand restraint might be one of the measures for coping with longer disruptions, but the EU states in its In-depth study of European Energy Security that the transport sector has to become more oil independent in order to decrease vulnerability. [235]

Gas

- The EU is quite dependent on import for Gas supply, about 60 % of the total demand comes from countries outside the EEA.
- The flexibility of transport infrastructure in terms of geographical location, the number and available capacity of pipelines and LNG terminals, underground storage and the way infrastructure is operated all play an important role in shaping the resilience of the gas sector.
- The commission In-depth study of European Energy Security point to a number of key problems in retaining the needed redundancy regarding gas storages. Examples mentioned are the current business model (excess supply yields storage-to-storage competition), winter-summer pricing spreads and a horizon of expectation based on previous years undermine incentives to prevent crisis situations.
- The in depth study of the SWD also states that if the gas supply would be disrupted in the EU, the underground storages would be mitigating but the delivery capacity of these would probably be limited during a sustained disruption due to its winter-summer cycle.[236]

[234] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 37

[235] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 37

[236] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 62

Nuclear

- The EU is quite dependent on import for uranium as well, but since there is a variety of countries to import from, which are considered reliable, the possibility of shortage seems unelikely.[237]

Inventory

Detection

*CIWIN

CIWIN has two main functionalities, one of them being a rapid alert system. The CIWIN portal has 11 specific sector areas, including Energy and Nuclear fuel-cycle industry.[238]

*The CSIRT Network

According to the NIS-directive, operators of critical services (of which Energy is one of the most important) must report cyber incidents to their national CSIRT or to their national authority handling cybersecurity – if they are severe enough to have significant impact on the continuity of the service in question. The information about the incident must be thorough enough for the CSIRT/authority to make an assessment of the possible cross border effect of the incident. The NIS-directive furthermore describes parameters for assessing the severity of impact from a cyber incident. [239] Those are;

- "(a) the number of users affected by the disruption of the essential service". [240]
- "(b) the duration of the incident;" [241]
- "(c) the geographical spread with regard to the area affected by the incident." [242]
- "(d) the extent of the disruption of the functioning of the service."[243]

The CSIRT or authority is then required to report to Member States who has essential services which might be significantly affected by the incident get information about it.[244]

[237] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 80
[238] Commission provisions on "ARGUS" general rapid alert system, 2005, p. 3
[239] The NIS-directive Brussels, 18 December 2015, 15229/2/15 REV 2, p. 39-40
[240] The NIS-directive Brussels, 18 December 2015 15229/2/15 REV 2, p. 39-40
[241] The NIS-directive Brussels, 18 December 2015 15229/2/15 REV 2, p. 39-40
[242] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 39-40
[243] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 43
[244] The NIS-directive Brussels, 18 December 2015 (OR. en) 15229/2/15 REV 2, p. 43

EU-Russia Early warning mechanism

Following a gas dispute between Russia and Ukraine in 2009, the EU and Russia established an Early Warning Mechanism in order to ensure rapid communication and prevent disruption in electricity, oil or gas.[245]

*European Community Urgent Radiological Information Exchange (ECURIE)

ECURIE (European Community Urgent Radiological Information Exchange) is a system implemented in 1987 intended to provide early notification and information exchange during radiological or nuclear emergency. In case of emergency the member states are required to report measures taken and levels of radiation at appropriate intervals. The system consists of three parts: CIS (Convention Information Structure) that defines both what information to send and in what format to send it, CoDecS (Coding Decoding Software) used to create as well as send and receive information in the CIS, lastly each Member State and the EC appoint a network of dedicated Contact Points (CPs) and Competent Authorities (CAs) who operate the system.

Radioactivity Environmental Monitoring (REM)

Integral to ECURIE are **REM (Radioactivity Environmental Monitoring).** In case of emergency (nuclear or radiological) support for exchange of essential data and information is provided by REM through ECURIE.

European Commission RAdioactive Discharges Database (RADD)

RADD is intended to collect, store, exchange, and disseminate information on radioactive discharges. In the case of a nuclear or radiological/nuclear emergency, REM provides support for the exchange of essential data and distributes messages notifying that an accident has happened. [246]

*European Radiological Data Exchange Platform (EURDEP)

There is also a real-time monitoring system called EURDEP (European Radiological Data Exchange Platform) that is automated and collects information in 37 European countries and redistributes this data to other relevant authorities, national and international.

The platforms main task is to alert and inform relevant authorities as well as the general public about the release of radioactivity in the atmosphere, during the early phase of an incident. The goal is to do this as fast as possible and to reach out as far as possible.[247]

Sensemaking

[245] http://ec.europa.eu/energy/en/topics/international-cooperation/russia
[246] https://rem.jrc.ec.europa.eu/RemWeb/Activities.aspx
[247] https://remon.jrc.ec.europa.eu/

ENSEMBLE

ENSEMBLE is a web-based platform for the inter-comparison and evaluation of atmospheric chemistry transport and dispersion models.

The system was originally developed for the support in case of nuclear emergencies and has evolved over time into a service to any kind of atmospheric model. ENSEMBLE can now be used for the inter-comparison and evaluation of models working at scales from local to global, and is capable of handling any number of variables and period of time.

Several are the activities in which ENSEMBLE has been used, ranging from data sets of monitoring data, in situ air quality, radiological meteorological data, vertical profiles and airborne data are available for a large number of case study. The ENSEMBLE system also allows users to perform on line ensemble analysis."[248]

European Nuclear Safety Regulators Group (ENSREG)

The European Nuclear Safety Regulators Group (ENSREG), an independent expert body, is the product of the Commission decision 2007/530/Euratom. ENSREG is intended to improve the conditions for, and reach common understandings regarding, nuclear safety and radioactive waste management. ENSREG also carry out stress tests, this is a practice induced by the Fukushima nuclear incident. This is a two-track process pertaining to safety and security, where safety is pertinent to ENSREG and refers to "extraordinary triggering events" (such as natural disasters) and how nuclear installations can withstand the consequences of such an event. The findings were summarised in a number of EU level reports in 2011, most importantly the need for preventive measures (such as hardened fixed equipment/bunkered equipment) but also on the response side (additional mobile equipment to mitigate severity of accidents and containment integrity) as well as periodic safety review. The security side pertains to "malevolent or terrorist acts" was handled by an Ad Hoc group on Nuclear Security (AHGNS) created by The Permanent Representatives Committee (COREPER). Its work is summarised in a report of its own, detailing good practices (32 all in all) and identifying a number of key themes: cyber/computer security, intentional aircraft crashes, synergy between safety and security and International Atomic Energy Agency's (IAEA) International Physical Protection Advisory Services (IPPAS) missions as well as exercises and training.

ENTSO-G exercises and stress-tests

Stress tests are carried out on a regular basis and are centred on scenarios based on horizon scanning, the intention is to create preparedness and detect possible threats to security of supply; highly pertinent seeing how the EU imports 53% of the energy used – 90% of its crude oil and 66% of its natural gas. The 2006 Russo-Ukrainian price dispute, and the resulting Russian cessation of gas deliveries, made it

[248] http://ensemble2.jrc.ec.europa.eu/public/?page_id=34

abundantly clear that the import dependent gas sector where parts of EU relied solely on Russian gas was of grave concern and the energy issue was suddenly on the centre stage. The ENTSO-G's mission is to facilitate and enhance cooperation between European transmission system operators (TSO) and guarantee the development of gas transmission systems, as regulated in the European Gas Regulation (EC) 715/2009.

The Incident and Threat Information Sharing EU Centre for the Energy Sector (ITIS-EUC)

The IT IS-EUC is an initiative by DG ENERGY and the portal is maintained by the JRC. The centre collects and shares information about emerging incidents in the energy sector in order to enhance situational awareness. One of the purposes of the IT IS-EUC is to provide a hub where operators within the energy sector may be informed about incidents as well as emerging threats and risks. It is possible that this function will be extended to involve more actors from other sectors in the future.[249] Besides providing information on emerging threats, the IT IS-EUC also analyses and distributes information on vulnerabilities to trusted partners within the energy sector, and furthermore works to enhance information sharing among stakeholders.[250]

*CIWIN

One of the main purposes with CIWIN is for Member States and stakeholders to exchange ideas, knowledge and best practices of CIP in order to enhance capability and raise awareness of CIP-issues. This happens with support of the CIWIN-portal. The portal "provides an IT tool that will facilitate CIP co-operation between Member States, that will offer an efficient and quick alternative to often time-consuming methods of searching for information, and that will offer Member States the possibility to communicate directly and upload information that they deem relevant".[251] It has multiple "areas", such as the "Member State-area", where each Member State can create its own space, and "Sector Areas", involving 11 sectors, including;

- Chemical Industry
- Energy

*The Thematic Network on Critical Energy Infrastructure Protection (TNCEIP)

The Thematic Network on Critical Energy Infrastructure Protection (TNCEIP) for the energy sector allows operators to exchange information on threat assessment, risk management and cyber security.[252]

[249] https://ec.europa.eu/jrc/en/scientific-tool/incident-and-threat-information-sharing-eu-centre-energy-sector-itis-euc

[250] https://ec.europa.eu/jrc/en/scientific-tool/incident-and-threat-information-sharing-eu-centre-energy-sector-itis-euc

[251] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008PC0676

[252] https://ec.europa.eu/energy/en/topics/infrastructure/protection-critical-infrastructure

On initiative of DG ENER and the Commission, TNCEIP consists of operators and owners of the energy infrastructure in the EU, including electricity, gas and oil. It aims to provide a common, comprehensive approach to protect transboundary energy infrastructure in Europe. Reportedly, all member have experienced a constant and increasing number of attacks on their energy infrastructures, including vandalism and cyberattacks. It furthermore aims to promote openness and information sharing between private-public actors within the sector as well as a common goal to work towards.[253]

*ENTSO-G

ENSTO-G also analyses resilience levels of in the Member States infrastructure, in order to determine the degree of flexibility during times of high demand. The energy infrastructure and its degree of flexibility is also connected to the gas storage and its deliverability, this since during times of high demand congestion may become a problem, however it's not elaborated on how this is to be solved outside of development of interconnectors and reverse flows.

Eastern Partnership Platform on Energy Security

The Eastern Partnership Platform on Energy Security brings together representatives from the EU, Armenia, Azerbaijan, Belarus, Georgia, Moldova, and Ukraine to discuss ways to promote energy security, renewable energy, energy efficiency, and nuclear safety. It also discusses the construction of missing infrastructure links and ways to bring partner countries' energy-related rules more in line with EU rules. The Platform meets twice a year.[254]

*Gas Infrastructure Europe (GIE)

Gas Infrastructure Europe (GIE) is a trusted partner of the EU institutions and bodies, and represents 68 member companies from 25 countries. The GIE supports the CIP measures of the Commission (as the Gas Transmission Network is one of "The four" focus sectors of the EPCIP) and the Member States such as GCG (Gas Coordination Group)-meetings, performing risk assessments, providing information and running stress-tests of energy security. [255]

*The GIE Security Risk Assessment Methodology

The GIE SRAM is a common approach to assess risks amongst the operators of European energy infrastructure. It assesses both threats and consequences of failure, and is available for all GIE members, as well as ENTSOG (the European Network of Transmission System Operators for Gas) and all other stakeholders interested in the field. It is described as an example of active participation of gas infrastructure operators to EPCIP.[256]

[253] Position Paper of the TNCEIP on EU Policy on Critical Energy Infrastructure Protection (November 2012), p.
[254] https://ec.europa.eu/energy/en/events/eastern-partnership-platform-energy-security
[255]
[256] GIE Security Risk Assessment Methodology, May 2015

Decisionmaking

Emergency stocks

Member States have various emergency response tools at their disposal, many of which are underpinned by EU legislation. Emergency stocks constitute the easiest and fastest way of making large volumes of additional oil and/or petroleum products available to an undersupplied market, thereby alleviating market shortage. The release of stocks can replace disrupted volumes and thereby it might be possible to avoid physical shortage and to dampen or eliminate potential price hikes. As a result, negative impacts of a disruption on the economy can be mitigated. The release of emergency stocks is now generally considered as the main emergency response tool to address an oil supply disruption (with other measures considered as supplementary to stock releases). EU Member States have to hold oil stocks for emergency purposes since 1968. The currently applicable Council Directive 2009/119/EC requires Member States to hold emergency stocks of crude oil and/or petroleum products equivalent to 90 days of net imports or 61 days of consumption, whichever is higher.

Should a supply crisis, a major disruption, occur the Commission is responsible for the organisation of a consultation between member states where it's to be determined how and where the emergency stocks should be used, hence the stocks cannot be moved prior to this consultation. However, there is a caveat regarding urgent situations where members states may release emergency and specific stocks in cases where this is necessary for an initial response, however what constitutes either a major disruption or a case of particular urgency is not expounded on. In Council Directive 2009/119/EC what is labelled specific stocks are introduced, these are stocks with a separate legal status that can be purchased by members states or the central stockholding entities (CSEs), in order to ensure that it is readily available in cases of particular urgency (in the form of disruption, not unfavourable price developments).

Demand Restraint

Another important emergency response tool is demand restraint. By reducing oil use in a sector in the short term, oil can be "freed up", thereby alleviating market shortage. Considering that most oil is used in transport, demand restraint measures typically target this sector. Such measures can range from light-handed measures like information campaigns encouraging people to use public transport to heavy-handed measures such as driving bans based on odd/even number plates. Most of these measures can be introduced at relatively low cost and at short notice but do require public acceptance (which may sometimes be difficult to obtain) and administrative control. In addition, extensive demand restraint may hamper economic activity and mobility. Demand restraint measures often have a limited impact (e.g. speed limit reductions) and/or take some time to have an impact on consumption (e.g. encouraging ecodriving). In a serious and prolonged disruption it will be necessary to ensure that certain groups of users (e.g. emergency services) are adequately supplied with petroleum products which might require the introduction of rationing/allocation schemes. According to EU legislation, Member States have to be able to reduce demand and allocate oil products in case of a disruption: Council Directive 2009/119/EC requires them to have procedures in place "to impose general or specific restrictions on consumption in line with the estimated shortages, inter alia, by allocating petroleum products to certain groups of users on a priority basis" (Article 19(1)). Fuel switching means the temporary replacement of oil by other fuels in certain sectors/uses. For example, oil used for electricity generation or for heating purposes may be replaced by other fuels, provided that technical systems are in place to allow the switch to the alternative fuel (e.g. natural gas). However, the actual potential to use fuel switching in a crisis is limited in most Member States. The majority of oil is now used in transport and in the petrochemical sector, where it is difficult or almost impossible to replace significant amounts of oil in the short term. In principle, a temporary increase of indigenous oil production can make additional oil available to the market. However, for technical and economic reasons, it is difficult to increase oil production at short notice. Only a handful of Member States produce oil in the EU and most of them have little or no spare capacity. By relaxing fuel specifications, the supply of certain petroleum products can be increased which, in principle, could contribute to alleviating a shortage. Under Directive 98/70/EC (fuel quality directive), the Commission may authorize higher limit values on the request of a Member State in case of “exceptional events, a sudden change in the supply of crude oils or petroleum products” (Article 7).

IEP (The International Energy Program) reallocation of oil

In case of disruption, the EU relies on. The IEA's founding treaty, the International Energy Program (IEP) also foresees the (re)allocation of oil in case of a severe supply disruption, drawing oil from countries that are less negatively affected to those which are more severely affected. This tool has never been applied in practice. In case of the disruption of supplies on a particular route, it may be possible to switch to alternative supply routes. This is particularly relevant for Member States and refineries supplied by pipelines. For example, the countries supplied by the Druzhba pipeline have the following alternative supply routes at their disposal: the Rostock-Schwedt pipeline (Germany), the Pomeranian Pipeline (Poland), the Ingolstadt-Kralupy (IKL) pipeline (Czech Republic) and the Adria pipeline (Hungary and Slovakia). However, some of these are not immediately available and/or have insufficient capacity to wholly replace the Druzhba pipeline. The oil-related "projects of common interest" (PCI) announced by the Commission in October 2013 would increase the capacity of these routes and/or would establish additional routes. Producing hydrogen using electricity generated from renewables, and using fuel cells that convert it back into electricity more efficiently than conventional technologies, can provide a solution. [257]

Coordination

The European Reference Network for Critical Infrastructure Protection (ERN-CIP)

Based under the Joint Research Centre, ERN-CIP (The European Reference Network for Critical Infrastructure Protection) aims at improving security solutions and linking capabilities by carrying out research, experiments and testing of technology and solutions for critical infrastructure protection. [258] The ERN-CIP-has thematic groups specifically focused on one aspect of CIP. For example;

- Chemical and Biological (CB) Risks to Drinking Water
- Radiological and Nuclear Threats to Critical Infrastructure
- Case Studies for Industrial Automation and Control Systems
- Industrial Automated Control Systems and Smart Grids[259]

Trans-European Energy Networks (TEN-E)

Since it has been established that modern infrastructure is crucial to reliable energy networks, the trans-European energy networks (TEN-E) was formed. The TEN-E list and rank relevant projects (i.e. if deemed eligible for Community assistance) based on three categories: priority projects, projects of common interest and projects of European interest. Projects of common interest and priority projects must display economic viability and in themselves help reinforce security of supply such as solve bottleneck problems and ensure interoperability (between systems and over state borders and thus enabling energy deliveries from more sources), while a project of European interest must also be of cross-border nature or have significant impact on cross-border transmission capacity.

Meaningmaking/Communication

*European Radiological Data Exchange Platform (EURDEP)

EURDEP aims to provide swift information to the public in case of release of radioactivity to the atmosphere.[260]

[257] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 112

[258] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/crisis-and-terrorism/critical-infrastructure/index_en.htm

[259] https://erncip-project.jrc.ec.europa.eu/

[260] https://remon.jrc.ec.europa.eu/

Accountability

*ENTSO-G analysis of disruption effects

ENTSO-G analyses and estimates impact effects of energy disruption in the EU by analyzing the response of the Gas infrastructures in a simulated crisis. Based on these estimates, lessons are drawn about the level of resilience, flexibility and overall response of EU Member States in case of a crisis.[261]

ENISA cyber exercise platform

The Cyber Exercise Platform is a not yet implemented initiative from ENISA, which aims to promote information sharing on cybersecurity exercises practises and lessons learned, as a step of building a cyber security exercise community. It will provide a platform where actors can publish information about their exercises and get access to information about others.[262] Exercises involving the energy-sector, and lessons learned from these exercises, will be included in the database.

Radioactivity Environmental Monitoring (REM)

Information about REM evaluations on various EU exercises and initiatives are located in the REM website archives, and includes for example;
EURANOS: European approach to nuclear and radiological emergency management and rehabilitation strategies (ended 2006).

The JRC's Major Accident Hazards Bureau (MAHB) ; eMARS Major Accident Database

The eMARS Major Accident Database is a collection of accident reports which contains events on chemical accidents. MAHB's research focuses on lessons learned studies to understand causes and trends in industrial accidents in the EU and worldwide as an aid to enforcement and monitoring national authorities and also as a general contribution to the study of industrial risks."[263]
Furthermore, the database also encompasses research on investigation, reporting and analytical methods for improving extraction of lessons learned that can broadly influence chemical accident prevention associated with particular substances, industry sectors, processes and equipment. The target

[261] COMMISSION STAFF WORKING DOCUMENT In-depth study of European Energy Security Accompanying the document Communication from the Commission to the Council and the European Parliament: European energy security strategy {COM(2014) 330 final}, p. 112
[262] https://www.enisa.europa.eu/topics/cyber-exercises/cyber-exercises-platform
[263] https://minerva.jrc.ec.europa.eu/en/content/minerva/c76dfa82-97a9-435f-8e0e-39a435aeec3a/who_we_are

audience is a diversity set of competent authorities and therefore, different analyses serve different communities.[264]

*Incident and Threat Information Sharing EU Centre for the Energy Sector - ITIS-EUC

One of the objectives of the IT IS-EUC is to analyse incidents, identify and share lessons learned for the energy sectors. ITIS-EUC aims to provide a service to its members and stakeholders through a dedicated office with the tasks to store and disseminate information on threats, vulnerabilities and incidents in the energy sector. [265]

[264] https://minerva.jrc.ec.europa.eu/en/content/minerva/f4cffe8e-6c6c-4c96-b483-217fe3cbf289/lessons_learned_from_major_accidents
[265] https://itis.jrc.ec.europa.eu/about

The Transport Sector

Introduction

General Background

The Council Directive 2008/114/EC of 8 December 2008 “on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection” defines the Transport sector as one of the two (the other one is energy) main European critical infrastructure sectors. The document defines the transport subsectors as following;

Sector	Subsector(s)
Transport	Road transport Rail transport Air transport Inland waterways transport Ocean and short-sea shipping and ports

Since the transport sector counts as one of the main CIP-sectors, EU legislation and measures for CIP is highly relevant for this sector. While each of the subsectors have their own crisis management, safety and security measures, and the overall transport sector is the responsibility of DG MOVE at the EU-level, the transport sector and its subsectors are also connected through CIP – which is the responsibility of DG Home. Besides, Space and Critical Information Infrastructure/cyber are two additional sectors which are linked to the functioning of the transport sector. Space infrastructure, more precisely the European Global Navigation Satellite Systems (GNSS), is essential for the functioning of transport activities.[266] Due to the dependence on digital services, the transport sector is also vulnerable to cyber threats, which DG Connect and agencies such as ENISA is responsible for. In conclusion, the crisis management measures of the transport sector with subsectors is quite complex, involving everything from subsectors individual measures to overall CIP measures, EU cybersecurity measures and generic crisis management structures.

[266] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, p.13

Policy Background

Critical Infrastructure Protection

- The EU has continuously funded a great amount of projects for improving CIP under the programme 'Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks' (CIPS) between 2007 and 2013, including;
- Risk assessment methodologies in air traffic management.
- Assessments of resilience of control management systems.
- Interactive risk assessments in critical infrastructures. [267]

- A review of EPCIP was made in 2012, taking into account opinions of Member States and relevant stakeholders. This review revealed that the cross-sector and cross-boundary links of CI were not given enough consideration. The review resulted in the '2013 Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection' which includes specifications on implementation activities of the prevention, preparedness and response-work streams. In the new approach, working with the chosen four CIs of the EU dimension is one of the highlighted measures. One of these four is **Eurocontrol**, which is the EU air traffic management Network.

- Moreover, the tools and processes to CIP and Critical infrastructure resilience used in the work with 'The Four' might, according to the document, be useful for other infrastructures of relevance. An additional objective of the Staff Working Document is to improve private-public dialogues on CIP. By implementing the new approach and focusing on 'The Four', the European Commission aims to support Member States individually as well as collectively regarding CIP. [268]
- Due to the identified need for enhanced network and information security of critical infrastructure sectors, the Network and Information Security Directive was proposed in 2013 along with the Cybersecurity Strategy of the EU. It states that sectors such as banking, energy, health, transmission and distribution**, transport,** public administrations and internet services play important roles for our society and economy, while being highly dependent on network

[267] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, p.7

[268] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, p. 3

and information systems (cyber). According to the NIS-directive, the companies in these critical sectors will be required to;[269]

- Report to the cybersecurity authorities (or CSIRT) cyber incidents that may significantly affect the continuity of critical services .[270]
- Assess and manage cyber risks.[271]

Expected implementation of the NIS-directive is August 2016.[272]

Air

- In 1980, the EU adopted the Directive 80/1266/EEC on cooperation and mutual assistance between the Member States in the field of air accident investigation. The Directive of 1980 was subsequently replaced by Directive 94/56/EC, which transposed into the EU legislation a number of principles contained in Annex 13 of the Chicago Convention.
- During 2002, the Regulation (EC) No 1592/2002 on common rules in the field of civil aviation was adopted, which also established the **European Aviation Safety Agency** .
- On May 2006, Regulation (EC) No 736/2006 on working methods of the European Aviation Safety Agency was adopted.
- In 2008, Regulation (EC) No 216/2008on common rules in the field of civil aviation and establishing a European Aviation Safety Agency replaced the initial framework Regulation N° 2320/2002 of the European Parliament and of the Council in order to meet evolving risks and to allow new technologies to be introduced.
  Commission Regulation (EU) N°72/2010 lays down procedures for conducting Commission inspections in the field of aviation security.
- In 2010, the European Commission conducted a comprehensive review of EU legislation on civil aviation accident and incident investigations. This review resulted in the adoption of Regulation (EU) No 996/2010 , which currently provides the legal framework for the conduct of civil aviation accident and incident investigations in the EU.
- Following the entry into force of Regulation (EU) No 996/2010, civil aviation safety investigation authorities of EU Member States gathered on 19 January 2011 in Brussels to establish the "European Network of Civil Aviation Safety Investigation Authorities" (ENCASIA).

[269] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

[270] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

[271] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

[272] Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union, REV 2, December 2015, p. 25

- Additionally, a European Central Repository of Safety Recommendations and their responses has been created, access to which is regulated by Commission Decision 2012/780/EU. [273]
- In 2016 the whole set of previous implementing legislation was updated: Commission implementing Regulation (EC) N° 2015/1998lays down detailed measures for the implementation of the common basic standards on aviation security.

Maritime

- In order to support Member States in case of pollution accidents, the EU set up the "Urgent Pollution Alert Section" in 1984. The Community Cooperation Framework (2000-2006) was established in order to support preparedness mechanisms in maritime accidents. [274]
- After the Erika incident 2002, EMSA (The European Maritime Safety Agency) was established by Regulation (EC) 1406/2002 . Subsequent amendments have enlarged its mandate (see Regulation (EU) 100/2013).[275]
- The EU legislation on maritime security consists of preventive measures such as the Regulation on enhancing ship and port facility security and the Directive on port security on the other hand.
- The Commission monitors the implementation of Maritime security legislation and evaluates the effectiveness of Member States Maritime security structures. In order to perform this task, the Commission has adopted a regulation on procedures for conducting Commission inspections in the field of maritime security.
- With the Third Maritime Safety Package adopted in 2009, the EU expanded its legislative arsenal covering all chains of responsibility in the maritime sector.
- Piracy is a major maritime security concern which is addressed in for example the Commission Recommendation of 11 March 2010 on measures for self-protection and the prevention of piracy and armed robbery against ships [2010/159/EU] .[276]
- Cleaning and recovery efforts after oil spill accidents can be extremely costly. The Helsinki and Barcelona conventions, as well as the Lisbon and Bonn Agreements are cooperation agreements to support recovery efforts. The EU participates in these agreeements.[277]

Other EU policy document on Maritime security;

[273] http://ec.europa.eu/transport/modes/air/safety/accident_investigation/index_en.htm
[274] http://ec.europa.eu/echo/what/civil-protection/response-to-marine-pollution_en
[275] http://ec.europa.eu/transport/modes/maritime/emsa/emsa_en.htm
[276] http://ec.europa.eu/transport/modes/maritime/security/index_en.htm
[277] http://ec.europa.eu/echo/what/civil-protection/response-to-marine-pollution_en

- Regulation (EC) No 725/2004 of the European Parliament and of the Council of 31 March 2004 on enhancing ship and port facility security
- Directive 2005/65/EC of the European Parliament and of the Council of 26 October 2005 on enhancing port security
- Report from the Commission to the Council and the European Parliament on transport security and its financing [COM/2006/0431 final]
- Commission Regulation (EC) No 324/2008 of 9 April 2008 laying down revised procedures for conducting Commission inspections in the field of maritime security
- Report assessing the implementation of the Directive on enhancing port security [COM(2009) 2]
- The Second report assessing the implementation of the Directive on enhancing port security [COM(2013) 792]

Land

- According to DG MOVE, there is "currently no EU legislation addressing land transport security (apart for dangerous goods where there is some overlap of safety and security requirements). Though it is noteworthy that in the 21st century the number of deaths in the EU from terrorist attacks on land transport far exceeds the number killed in aviation or maritime, and theft of cargo from road and rail is estimated to cost some €8 billion per year, EU Transport Ministers have, to date, not requested the Commission to bring forward any legislation for EU security requirements for either road or rail transport."[278]
- "In 2012, the Commission adopted a Staff Working Document on Transport Security, which highlighted the lack of EU legislation in land transport security and made suggestions of possible areas where EU action could add value. In the first instance an **EU Expert Group for Land Transport Security** was set up in order to have a forum to discuss issues with both Member States and stakeholders."[279]
- One of the reasons to the lack of rules and policies in land transport is that the threats and risks are quite diverse, which makes it tough to design policies that fits all and the responsibility of legislation falls down sector by sector instead.[280]

[278] http://ec.europa.eu/transport/themes/security/land_security_en.htm
[279] http://ec.europa.eu/transport/themes/security/land_security_en.htm
[280] http://ec.europa.eu/transport/themes/security/land_security_en.htm

Earlier Incidents/crises

Eyjafjallajökull volcano ash cloud (air)

In 2010, the volcano eruption on Iceland and the following ash cloud demonstrated the vulnerability of the European aviation system, and made the lack of functioning of emergency procedures clear. However, the EU, led by the Commission with support of EUROCONTROL, used the lessons learned in order to make swift institutional change and establish the European Aviation Crisis Coordination Cell (EACCC) under the responsibility of the Network Manager (EUROCONTROL).[281]

ERIKA & Prestige accidents (maritime)

The Erika and Prestige were oil spill accidents. When ERIKA sank in December 1999 outside the French western coast it spilled 20,000 tons of heavy fuel oil. PRESTIGE sank three years later, spilling 70,000 ton of oil. The accidents caused the EU to reform and adopt new rules to prevent maritime accidents. With the support of the European Maritime Safety Agency (EMSA), the Commission focuses on the EU Member States proper implementation of EU Maritime safety regulation.

Institutional Landscape

DG Home (Critical Infrastructure Protection)

DG MOVE

EUROCONTROL

Eurocontrol is not an EU agency, but the EU Air Traffic Management Network, an intergovernmental organization of 41 states. However, in 2011, the EU nominated Eurocontrol as the European Network Manager, and is in close cooperation to the Commission and the EU in many ways. For example, the EACCC (European Aviation Crisis Coordination Cell) was established in 2010 as a joint initiative of Eurocontrol and the Commission to coordinate the management of crisis response in the ATM network. Also, Eurocontrol is one of “The Four” chosen CI’s of EPCIP.

Eurocontrol’s tasks includes;

- Providing operational and technical expertise.
- Advisory services, both military and civilian.
- Coordination among states.
- Training and simulations.

[281] http://ec.europa.eu/transport/modes/air/single_european_sky/eaccc_en.htm

- Information exchange.
- Civil-military cooperation. [282]

The European Railway Agency (ERA)

ERA was set up in 2006 with the objective of building an integrated European railway area and promoting rail safety as well as interoperability. ERA is based in France and works closely with EU institutions. Among its tasks are;

- To develop common technical specifications as well as common safety approaches.
- To monitor and report on rail safety in the EU.[283]
- To develop a common European training programme for investigators.
- To coordinate accident investigation.[284]

European Maritime Safety Agency (EMSA)

EMSA was set up 2002 as a measure after the “Erika” accident. Among the tasks of EMSA are;

- To assist the Commission in the fields of maritime security, safety and environmental issues.
- To assist the Commission in updating and developing Maritime legislation and monitor as well as evaluating its implementation.
- To perform inspections in Member States.
- To assist Member States with implementation of EU legislation.
- To organize training activities and support information exchange. [285]

The Agency also provides satellite imagery for detection and monitoring of oil spills, pollution response experts to give operational and technical assistance, and information service for chemical spills at sea.

Subsectors

Connected subsectors: Satellite system/Cyber

Space and Critical Information Infrastructure/cyber are two sectors which are linked to the functioning of the other subsectors. Space infrastructure, more precisely the European Global Navigation Satellite

[282] http://www.eurocontrol.int/articles/who-we-are
[283] http://ec.europa.eu/transport/modes/rail/interoperability/index_en.htm
[284] http://www.era.europa.eu/Core-Activities/Safety/Accident-Investigation/Pages/Maintenance.aspx
[285] http://ec.europa.eu/transport/modes/maritime/safety/emsa_en.htm

Systems (GNSS), is essential for the functioning of activities such as telecommunications, transport and trade.[286]

Cyber security and critical information infrastructure becomes an important aspect of transport security since it the sector rely on cyber for its services, thus becoming vulnerable to cyber threats which may hinder;

- “Confidentiality – unauthorized access to or interception of information.” [287]
- “Integrity – unauthorized modification of information, software, physical assets.” [288]
- “Availability – blockage of data transmission and/or making systems unavailable.” [289]

“Galileo is the European Global Navigation Satellite Systems (GNSS) – which is the first EU owned Space Infrastructure. A major failure, whether accidental or intentional, of such GNSS infrastructure will impact the users but also affect many other critical infrastructures in which GNSS services are already deeply integrated: **Transport**, telecommunications, trade and banking activities rely on GNSS signals for timing, navigation and secure transactions. GNSS signals can be subject to a number of threats on the radiofrequency links such as interference, unauthorised access and misuse, jamming, falsification and cyber-attacks”. [290]

Inventory

Detection

Eurocontrol Pilot-In-Flight Reports

Pilot-in-Flight Reports, detects and observs threats such as ash-clouds. [291]

*Galileo Security Monitoring Centre (GSMC)

Galileo Security Monitoring Centre (GSMC) monitors security threats, manages security alerts and monitors the functioning of the systems components. [292]

[286] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, p.13
[287] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf
[288] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf
[289] https://ec.europa.eu/energy/sites/ener/files/documents/EECSP%20_%20CfE__FINAL.pdf
[290] Brussels, 28.8.2013 - COMMISSION STAFF WORKING DOCUMENT on a new approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures more secure, p.13
[291] http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010
[292] http://www.gsa.europa.eu/security/gsmc

SafeSeaNet

SafeSeaNet is a vessel traffic monitoring and information system for European waters. It is operated by EMSA together with Member States and in cooperation with the Commission. It identifies and tracks vessels by their **Tracking Automatic Identification System (AIS)** and provides near real-time information about their positions and other status information. By doing so, it supports EU reporting services. The information provided by SafeSeaNet could be, for example;

- hazardous goods
- the number of people on board
- past positions of ships
- ships with high risk profiles
- accidents and incidents
- estimated or actual arrival and departure times in ports.
- Tracking vessels outside the range of AIS coastal networks requires the use of satellites.

The EU Long-Range Identification and Tracking (LRIT) Cooperative Data Centre

LRIT is an international tracking system for vessels. EMSA operates the EU LRIT Cooperative Data Centre, which covers 35 countries. The LRIT system was originally intended for maritime security purposes, but now includes areas such as maritime safety and Search & Rescue operations. The system gets information from vessels through satellites.[293] Except for monitoring vessels, the Centre can exchange information with other monitoring centres around the world. The EU LRIT CDC tracks 8000 ships every day.[294]

*Eurocontrol Network Operations Portal (NOP)

The Network Operations Portal (NOP) is an internet portal which brings together a number of Eurocontrol tools and provides instant information about air traffic operations for air professionals to use. One of its main purposes is monitoring (including capacity management measures). The portal allows users (both civil and military) to react to events faster, monitor performance and report functionality (or non-functionality). [295]

SECRET (Security of Railways against electromagnetic attacks) Detection Sensors

Since railways increasingly use wireless connection, the likelihood for communication jammers to be used in order to disrupt or damage railway communication has grown. Therefore, The SECRET

[293] http://www.emsa.europa.eu/operations/vessel-reporting-services.html
[294] http://www.emsa.europa.eu/lrit-home/lrit-home.html
[295] https://www.eurocontrol.int/articles/tools-available

detection sensors were developed in order to make it possible to detect an electromagnetic attack on railways both fast and with certainty.[296]

Sensemaking

*The Air Traffic Management Network Manager (NM)

The Network Manager is a centralized function for the EU created by the Commission. It functions as a hub for different actors in aviation and traffic management who are involved with management and planning of the ATM(air traffic management)-network.[297] Eurocontrol is the nominated Network Manager from 2011 until the end of 2019. During an event which could possibly affect the European aviation network negatively, the Network Manager receives a warning, gathers information and monitors the situation further. The NM assesses what information should go on the Network Operations Portal, and also decides on facilitating information exchange through, for example, teleconferences. [298] Among the tasks of the Network Manager is to foster partnership and operational cooperation (for example cooperative decision-making).[299] If a disruption of air traffic becomes major, the Network Manager moves from pre-alert to the disruption management phase. It continues to be an information hub and closely follows the development. It also decides what information should be distributed through the Network Operation Portal. Depending on the development of the situation, the NM may move back to pre-alert phase or to the crisis management phase, where it also activates the EACCC. During the crisis management phase, the Network Manager assists to mitigate the impact by, for example, providing situational awareness, tools and services for actors to react more efficiently. [300]

CIWIN portal: transport

One of the main purposes with CIWIN is for Member States and stakeholders to exchange ideas, knowledge and best practices of CIP in order to enhance capability and raise awareness of CIP-issues. This happens with support of the CIWIN-portal. The portal "provides an IT tool that will facilitate CIP co-operation between Member States, that will offer an efficient and quick alternative to often time-consuming methods of searching for information, and that will offer Member States the possibility to communicate directly and upload information that they deem relevant".[301] It has multiple "areas", such

[296] http://cordis.europa.eu/news/rcn/123444_en.html
[297] http://www.eurocontrol.int/faq/corporate
[298] http://www.eurocontrol.int/articles/disruptions-and-crisis-management
[299] https://www.eurocontrol.int/articles/network-manager-governance-and-functions
[300] https://www.eurocontrol.int/articles/network-manager-governance-and-functions
[301] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008PC0676

as the "Member State-area", where each Member State can create its own space, and "Sector Areas", involving 11 sectors, including **Transport**. [302]

*Eurocontrol Network Operations Portal (NOP)

The Network Operations Portal allows practitioners to increase their knowledge of the air situation and plan collaborative air operations from strategic to tactical levels, increasing efficiency and collaboration capacity.[303] The NOP serves two main purposes. One is monitoring airspace and capacity as well as planning pan-European operations and utilizing the collaborative ATM capacity. [304] The other one is to enable partners to anticipate or react to disruptive events more effectively. By offering an updated situational picture, it improves decision making during a time of crisis.[305]

European Network of Civil Aviation Safety Investigation Authorities (ENCASIA)

ENCASIA consists of EU Member State air safety authorities. Its establishment is based in the Regulation (EU) 996/2010 on the investigation and prevention of accidents and incidents in civil aviation, which entered into force on 2 December 2010. ENCASIA aims to support the development of training activities, safety investigation best practices and sharing resources. ENCASIA also advices the EU institutions on air incident prevention and investigation.[306]

The Maritime Security Committee (MARSEC)

MARSEC seeks to support the Commission with specific focus on its activities under Directive 2005/65/EC. MARSEC is a forum chaired by the Commission and consisting of Member State experts. The forum discusses maritime security issues, shares best practices and indicators. The committee has developed a mechanism for secure mutual information sharing (on sensitive information), including threat evaluations. [307]

The Stakeholder Advisory Group on Maritime Security (SAGMaS)

The Stakeholder Advisory Group on Maritime Security is a forum where stakeholders discuss the work of MARSEC. The Commission has regular meetings with SAGMaS, and any organization of stakeholders related to Maritime security can be invited.[308]

The European Rail Agency's harmonized Safety Management System (SMS)

- Ensures risk management of infrastructure managers regarding railway undertakings.

[302] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52008PC0676
[303] https://www.eurocontrol.int/articles/tools-available
[304] http://www.eurocontrol.int/articles/tools-available
[305] http://www.eurocontrol.int/articles/tools-available
[306] http://ec.europa.eu/transport/modes/air/encasia/index_en.htm
[307] EU legislation on Maritime Security framework
[308] EU legislation on Maritime Security framework

- Provides a methodology for monitoring safety requirements.[309]

The European Rail Agency's NIB Network

- Consists of national investigation bodies that meet a couple of times a year in order to exchange views and experiences with topics such as common investigation methods. Often, ERA work with smaller task forces on issues such as safety recommendations and training.[310]

*European Aviation Crisis Coordination Cell (EACCC)

In the event of crisis, the EACCC acts as an information hub and organizes conferences involving experts, its members as well as state focal points. Based on the assessment of the situation, it distributes communications to the Commission, EASA, Eurocontrol, the Network Manager, civil and military authorities, etc.[311]

During the crisis management process, the EACCC collects, analyzes and distributes information to generate a common situational picture and situational awareness among the aviation community.[312]

*EVITA

EVITA is one of the Network Operations Portal's features - an online tool which was originally created to monitor ash clouds, but has developed to be used for crises caused by for example pandemics or nuclear emergencies. It works by visualizing the impact of various crises in aviation/air traffic and on the air network in Europe. For example, it allows airlines to calculate which of their aircrafts will be affected by an ash-cloud. Its functions support decision-makers during a crisis as well as information sharing between relevant actors such as airlines, state regulators and air navigation. It counts as the principal communication channel for airlines in Europe during a major crisis. [313]

European Maritime Safety Agency (EMSA)

Besides providing detection-systems for oil spill accidents, EMSA also provide pollution response experts to give advice and assistance during the response phase, and also distribute information on chemical spills.[314]

[309] http://www.era.europa.eu/Core-Activities/Safety/Safety-Management-System/Pages/Csm-On-Monitoring.aspx
[310] http://www.era.europa.eu/Core-Activities/Safety/Accident-Investigation/Pages/Networking.aspx
[311] http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010
[312] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc
[313] http://www.eurocontrol.int/articles/tools-available
[314] http://ec.europa.eu/echo/what/civil-protection/response-to-marine-pollution_en

Decisionmaking

*European Aviation Crisis Coordination Cell (EACCC)

In the event of a crisis:

- The EACCC chairperson contacts the relevant State Focal Points and those at risk at the beginning of any crisis, as well as relevant expert organisations, depending on the type of crisis. [315]
- The EACCC is then convened via meetings or teleconferences, and the State Focal Points contacted. [316]
- Then, a crisis-mitigation policy is discussed, agreed and approved by the EACCC. The State Focal Points provides the necessary link to the national level actions. [317]

*The Air Traffic Management Network Manager

If a disruption of air traffic becomes major, the Network Manager moves from pre-alert to the disruption management phase. It continues to be an information hub and closely follows the development. It also decides what information should be distributed through the Network Operation Portal. Depending on the development of the situation, the NM may move back to pre-alert phase or to the crisis management phase, where it also activates the EACCC. During the crisis management phase, the Network Manager assists to mitigate the impact by, for example, providing situational awareness, tools and services for actors to react more efficiently. The Network Manager has developed a network disruptions management procedure, which was aligned with the NM IR and published in summer 2011, in order to support the EACCC. In case of a crisis (which could be caused by for example volcanic ash, a pandemic or a massive cyber-attack) the **Network Manager Operations Centre** (NMOC) monitors and coordinates the measures taken in response.[318] The NMOC (previously called Central Flow Management Unit /CFMU) performs both crisis and contingency management as well as post-operations analysis.[319]

[315] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc
[316] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc
[317] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc
[318] http://www.eurocontrol.int/articles/disruptions-and-crisis-management
[319] https://www.eurocontrol.int/network-operations

Coordination

The Civil Protection Mechanism/ERCC: Marine pollution emergency response

The ERCC has the capacity to assist during a marine pollution accident, for example by gather and coordinate supporting expertise from both EMSA and participating states and by mobilizing oil recovery measures.[320]

European Maritime Safety Agency (EMSA)

During an oil-spill accident by sea, EMSA can upon request mobilize commercial normal vessels in the regional seas of Europe to cease their ordinary activities and become oil spill recovery vessels.[321]

*European Aviation Crisis Coordination Cell (EACCC)

In the event of network crisis, the Network Manager, with the support of the European Aviation Crisis Coordination Cell (EACCC) is responsible for coordinating the management of response to the network crisis, involving close cooperation with corresponding structures in Member States.

During a crisis, the EACCC proposes and takes crisis response initiatives and coordinates information flows between decision makers, airspace users and service providers.[322]

*EACCC: Volcanic Ash Crisis Exercises (VOLCEX)

The EACCC is used to conducting exercises to maintain the high level of preparedness for possible crisis events. Crisis exercises dealing with volcano ash clouds, cyber-security and nuclear incidents have already taken place. [323] For example, the **Volcanic Ash Crisis Exercises (VOLCEX),** which is Annual simulation exercises to test the European Aviation Crisis Coordnation Cell and the European Crisis Visualization Interactive Tool for ATFCM (EVITA). [324]

*EVITA

EVITA allows airlines to calculate which of their aircrafts will be affected by an ash-cloud. EVITA support decision-makers during a crisis as well as the information sharing between relevant entities such as airlines, state regulators and air navigation. EVITA is one of the principal communication channel for airlines in Europe during a major crisis. [325]

[320] http://ec.europa.eu/echo/what/civil-protection/response-to-marine-pollution_en
[321] http://ec.europa.eu/echo/what/civil-protection/response-to-marine-pollution_en
[322] http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010
[323323] http://ec.europa.eu/transport/modes/air/single_european_sky/eaccc_en.htm
[324] http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010
[325] http://www.eurocontrol.int/articles/tools-available

*The Air Traffic Management Network Manager (NM)

The Network Manager is a centralized function for the EU created by the Commission. It functions as a hub for different actors in aviation and traffic management who are involved with management and planning of the ATM(air traffic management)-network with the aim to make the network run as smoothly as possible under any circumstances. [326] Eurocontrol is the nominated Network Manager from 2011 until the end of 2019, when it will seek re-designation. The ATM Network includes the 28 Member States of the EU as well as all of Eurocontrol's members and others according to agreements.

Among the events which could raise the alert-levels of the Network Manager are;

- Bad weather;
- Industrial action;
- Volcanic eruption;
- Armed conflict;
- Security incidents;
- Nuclear accident;
- Staff shortages;
- Uncontrolled re-entry of satellites.

*Network Manager Operations Centre

In case of a crisis (which could be caused by for example volcanic ash, a pandemic or a massive cyber-attack) the **Network Manager Operations Centre** (NMOC) monitors and coordinates the measures taken in response.[327] The NMOC (previously called Central Flow Management Unit /CFMU) performs both crisis and contingency management as well as post-operations analysis.[328]

[326] http://www.eurocontrol.int/faq/corporate
[327] http://www.eurocontrol.int/articles/disruptions-and-crisis-management
[328] https://www.eurocontrol.int/network-operations

Meaningmaking/Communication

*European Aviation Crisis Coordination Cell (EACCC)

During a crisis, the EACCC distributes and mannages communications to the Commission, EASA, Eurocontrol, the Network Manager, civil and military authorities.[329]

The EACCC also manages communication through a nominated communications focal point, in order to ensure a consistent message based on the situational assessment made. This is transmitted to the Network Manager (Eurocontrol/EC/EASA) as well as other relevant civilian and military actors.[330]

*The Galileo Public Regulated Service

The PRS is a service which ensures continuity, more specifically service to authorized users when access is denied to other navigation services. It provides a protected signal for critical application. The PRS can be useful for EU public safety and emergency services. [331]

Accountability

*EACCC Lessons learned session

Since the EACCC is mainly tasked to manage crises at the response-phase, it is not focused at learning or recovery. When a crisis is assessed to be resolved, the EACCC is deactivated. However, in order to address remaining actions and identify lessons learned, a debriefing EACCC-session is held.[332]

*European Maritime Safety Agency (EMSA)

EMSA is the secretariat for the Permanent Cooperation Framework of Accident Investigation Bodies. It is responsible for assisting the implementation of Directive 2009/18/EC which establishes the principles of accident investigation in the maritime sector. EMSA is also responsible for EMCIP, the European Marine Casualty Information Platform. Among EMSA's recovery-tasks are also;

- To support activities to develop Member States accident investigation capabilities.
- To support the ability to collect and analyze casualty data at the EU-level.
- To verify EMCIP data.
- To provide operational support to Member States (if requested) during marine accident investigations.
- To analyze marine casualty data and reports.

[329] http://www.eurocontrol.int/articles/what-has-changed-aviation-dealing-volcanic-ash-2010
[330] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc
[331] http://www.gsa.europa.eu/security/prs
[332] http://www.eurocontrol.int/articles/european-aviation-crisis-coordination-cell-eaccc

- To publish the marine casualty and incident annual overview.[333]

*EASA

The agency has several tasks when it comes to accident and incident investigation support, such as;

- To support investigations with technical expertise.
- To monitor the progress of aircraft incident investigations.
- To provide reports on Safety Recommendations.
- To cooperate closely with European Accident Investigation Bodies.
- To establish corrective actions for identified safety deficiencies.[334]

The European Marine Casualty Information Platform (EMCIP)

A database and system operated by EMSA on behalf of the Commission and Member States, the EMCIPs main tasks are;

- To improve safety investigations.
- To improve analysis of the results of casualty investigations.
- To provide means for risk identification

Since 2011, incident reporting (including data resulting from investigation) has been mandatory for Member States. This has allowed EMSA to achieve new proposals for safety recommendations and improvements of existing legislation. EMCIP stores information regarding marine casualties, including all types of ships. The information collected in the system allows analysis of a variation of factors involved in marine accidents and incidents, including human errors, environmental factors, organizational factors and technical errors. Member States are data providers in the system, and the system supports their notification, reporting and searching tasks. The database has a common taxonomy, developed by EMSA and Member States. [335]

EMCIP holds a portal where investigators from around the EU may share information about incidents. Here, information about marine incidents is also published for the general public, for example through reports. The database is hosted by the JRC.[336]

[333] http://www.emsa.europa.eu/implementation-tasks/accident-investigation.html
[334] https://www.easa.europa.eu/easa-and-you/safety-management/accident-and-incident-investigation-support
[335] https://emcipportal.jrc.ec.europa.eu/index.php?id=83
[336] http://www.emsa.europa.eu/emcip.html

European Maritime Safety Agency Permanent Cooperation Framework (PCF)

The Permanent Cooperation Framework is an operational forum established by Member States in close partnership with the Commission. It allows Member States' maritime incident investigation bodies to cooperate, and it enables EMSA to facilitate cooperation required by its founding regulation. Notes from the PFC meetings are usually published on the European Casualty Information Platform (EMCIP).

The Health Sector

Introduction

General background

In the modern society, cross border health threats such as communicable diseases, chemical and biological events could spread quickly. Just like in other sectors, actual events has sparked development of new prevent and response measures at the EU-level. For example, the EU Health Security Committee was set up by the EU health Ministers in 2001 after the terrorist attacks and the deliberate release of anthrax toxins in the US.

The EU action regarding health has focused on general coordination, coordination of information , measures to combat communicable diseases and substances related to chemical, biological and radio-nuclear agents. Since 2005, the European Centre for Disease Prevention and Control has been working on risk assessments and supports the technical and scientific prevention/response of communicable diseases in Europe.[337]

Being a cross border threat, priority is to increase the preparedness at national level in all member states, that national plans are developed and that the EU dimension is considered. Moreover, interoperability of these plans is an important objective and is supported through coordination mechanisms and communication tools.[338]

Policy Background

- The 2008-2013 Health programme of the EU came into force on 1 January 2008 with the objective "to complement, support and add value to the policies of the Member States and contribute to increase solidarity and prosperity in the European Union by protecting and promoting human health and safety and by improving public health."[339]
- The Justice and Home Affairs Council adopted on 6 December 2007 Conclusions 'on addressing chemical, biological, radiological and nuclear risks and on bio-preparedness.
- The comprehensive EU strategy "Together for health" was adopted in 2007 in order to responds to challenges faced by member countries by strengthening cooperation and coordination across the EU.[340]
- On 24 June 2009 the Commission adopted a Communication on 'Strengthening Chemical, Biological, Radiological and Nuclear Security in the European Union' with an EU CBRN

[337] http://ec.europa.eu/health/preparedness_response/docs/commission_staff_healthsecurity_en.pdf
[338] http://ec.europa.eu/health/preparedness_response/preparedness/index_en.htm
[339] http://ec.europa.eu/health/programme/policy/2008-2013/index_en.htm
[340] http://ec.europa.eu/health/strategy/policy/index_en.htm

Action Plan,including recommendations in the areas of prevention, detection and response. A significant amount of financial resources (up to €100 million) was allocated to its implementation. The Communication was accompanied by a Commission Staff Working Document 'Bridging security and health: Towards the identification of good practices in the response to CBRN incidents and the security of CBR substances'.

- In April 2009 the European Commission adopted a three-year programme (2009–2011) to fight terrorism, trafficking and proliferation of weapons of mass destruction, including chemical, biological, radiological and nuclear (CBRN) materials.
- On 22 October 2013, the EU adopted a Decision to improve preparedness across the EU and strengthen the capacity to coordinate response to health emergencies. This Decision entered into force on 6 November 2013. The 2013 decision aimed at strengthen EU level planning capacity by coordination and improved information sharing of health security actions at the member state level. As many health threats are transboundary, ensuring a sufficient level of preparedness of all member states becomes even more important. Therefore, the decision describe that member states shall every three years (starting from 2014) give the Commission an update on ;
    - " identification of, and update on the status of the implementation of, the core capacity standards for preparedness and response planning as determined at national level for the health sector, as provided to the WHO in accordance with IHR;
    - description of the measures or arrangements aimed at ensuring interoperability between the health sector and other sectors including the veterinary sector, that are identified as being critical in the case of an emergency, in particular: (i) coordination structures in place for cross-sectoral incidents; (ii) emergency operational centres (crisis centres); (c) description of the business continuity plans, measures or arrangements aimed at ensuring the continuous delivery of critical services and products.The obligation to provide the information referred to in points (b) and (c) shall only apply if such measures or arrangements are in place or are provided for as part of national preparedness and response planning".[341]

Moreover, the 2013 document aimed to improve risk assessments regarding health threats. Recognizing its important role in the coordination of previous crises, the Health Security Committee was consolidated legally as a coordinator of health security preparedness, as well as a response manager (including communication with the public and decision of coordination

[341] DECISION No 1082/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC

of national responses in case of a crisis).[342] According to the 2013 Decision, experiences confirm the added value of coordinated EU action regarding health threat monitoring and early warning. The 2013 Decision also confirmed the adoption of the integrated all-hazards approach of the WHO.A report on the implementation of the Decision was adopted on 7 December 2015.[343]

- Third health programme (2014-2020) has four main objectives;

- Promote health, prevent diseases and foster supportive environments for healthy lifestyles taking into account the 'health in all policies' principle,
- Protect Union citizens from serious cross-border health threats,
- Contribute to innovative, efficient and sustainable health systems,
- Facilitate access to better and safer healthcare for Union citizens.[344]

Institutional landscape

- **DG SANCO**

Agencies:

- **European Centre of Disease Prevention and Control (ECDC)**

The European Centre of Disease Prevention and Control (ECDC) was established in 2005. It is an EU agency with aim to strengthen Europe's defences against infectious diseases. It is seated in Stockholm, Sweden.

- **European Medicines Agency (EMEA)**
- **European Food Safety Authority (EFSA)**

Earlier health threats

- **Ebola outbreak (2014-2015)**

The Ebola epidemic that emerged in West Africa in March 2014 – and declared a Public Health Event of International Concern by WHO in August 2014 – was the first emergency event addressed by ECDC andits partners under Decision 1082/2013 and SMAP.

- **Polio and MeRs outbreaks (2014-2015)**
- **Pandemic H1N1 (2009)**
- **Refugees / Migration following unrest in North African countries (2011)**

[342] http://ec.europa.eu/health/preparedness_response/policy/decision/index_en.htm
[343] http://ec.europa.eu/health/preparedness_response/docs/commission_staff_healthsecurity_en.pdf
[344] http://ec.europa.eu/health/programme/policy/index_en.htm

- **Volcano ash cloud (2010)**
- **Shortage of radio-isotopes used for medical purpose in the EU (2008)**

Inventory

Detection

*European Centre of Disease Prevention and Control (ECDC)

Included in the ECDC's mission is to identify and communicate current and emerging threats to human health posed by infectious diseases. It cooperates with various European national health protection entities to improve and develop early warning and monitoring systems that covers the whole continent.[345]

*RAS CHEM

RAS-CHEM is a detection and rapid alert system for chemical incidents. While RAS-BICHAT is only focused on terrorist activities, this early warning system covers accidental events as well and all public health aspects. It identifies and rapidly distributes information on chemical incidents, illnesses caused by chemical exposure etc. [346]

*RAS BICHAT

Rapid Alert System on Biological and Chemical Attack (RAS-BICHAT) manages rapid alerts due to terrorist attacks involving chemical, biological and radio-nuclear agents (CBRN). The primary target group is Health Security Committee members. RAS BICHAT is part of the Programme of cooperation on preparedness and response to biological and chemical agent attacks. Like RAS-CHEM, RAS-BICHAT is web-based and performs detection, early warnings. The Commission is moderator, unlike with the EWRS-system. [347]

Threat Tracking Tool (TTT)

The Threat Tracking Tool (TTT) is a database developed by the ECDC. Its task is to monitor verified health threat events, and supports the activities of the ECDC linked to these verified events. [348]

*The Epidemic Intelligence Information System (EPIS) early warning systems

EPIS has several early warning/detection platforms;

[345] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf
[346] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[347] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[348] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx

FWD (Food- and Waterborne Diseases and Zoonoses)

EPIS-FWD manages early warnings regarding outbreaks of food and waterborne diseases. Included in the platform are epidemiologists and microbiologists from all EU member states plus 16 non EU countries. [349]

STI (Sexually Transmitted Infections)

EPIS-STI manages early warning regarding STI in the EU. The nominated contact points for STI monitoring in EU/EEA countries can submit reports to EPIS-STI. [350]

ELDSNet (European Legionnaires' Disease Surveillance Network)

"EPIS-ELDSNet brings together data on Legionnaires' disease, with a focus on the detection and follow-up of travel-associated clusters, and the investigation of community outbreaks (in an ad hoc fora with restricted access)."[351]

VPD (Vaccine Preventable Diseases)

"EPIS-VPD facilitates the early detection and sharing of information on outbreaks of VPDs and adverse events from vaccinations, and allows exchange of information on technical topics related to vaccinations and the control of vaccine preventable diseases. The platform connects vaccination programme managers, vaccine experts, epidemiologists and microbiologists from the 31 EU/EEA Member States." [352]

AMR-HAI (Antimicrobial Resistance and Healthcare-associated Infections)

"EPIS-AMR-HAI supports the rapid reporting and dissemination of information related to bacterial pathogens with previously unseen or emerging antimicrobial resistance and healthcare-associated infections which are or may become relevant for public health within the EU/EEA. All 31 EU/EEA Member States have access to EPIS-AMR-HAI." [353]

The Early Warning and Response System (EWRS)

EWRS is a confidential computer system used for early warnings and alerts regarding communicable diseases with potential impact on the EU. The system connects member state public health authorities with the Commission and the European Centre for Diseases Prevention and Control (ECDC). The

[349] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[350] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[351] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[352] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[353] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx

EWRS also include EEA countries. Members should report events which might affect public health, such as outbreaks. The system is hosted by the European Centre for Disease Control (ECDC) and has close links to the WHO. The ECDC performs risk assessments based on the information coming in through EWRS. The EWRS has been successfully tested in a number of outbreaks such as the Pandemic Influenza A (H1N1) .[354]

According to the Decision on serious cross-border threats to health from 2013, threats which fulfils the following criteria shall be reported to the EWRS;

"(a) it is unusual or unexpected for the given place and time, or
it causes or may cause significant morbidity or mortality in
humans, or it grows rapidly or may grow rapidly in scale, or
it exceeds or may exceed national response capacity; and
(b) it affects or may affect more than one Member State; and
(c) it requires or may require a coordinated response at Union
level."[355]

Moreover, when member states notify the WHO of events that may constitute public health emergencies of international concern, they shall before or at the same time report an alert in the EWRS. When the alert is notified, the reporting competent national authority and the Commission shall provide as much information as possible of the event which might help coordination of response action. [356]

*Emerging Viral Diseases-Expert Laboratory Network (EVD LabNet)

The EVD-LabNet (**E**merging **V**iral **D**iseases-Expert **Lab**oratory **Net**work) focuses on detection and monitoring of viral diseases in Europe, especially re-emerging vector-borne viral infectious diseases.[357]

*The European Surveillance System (TESSy)

TESSy is a database hosted by the ECDC, providing a technical platform for monitoring/surveillance of communicable diseases in Europe.[358]

[354] http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/rapid_alert_en.htm

[355] DECISION No 1082/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC

[356] DECISION No 1082/2013/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC

[357]http://ecdc.europa.eu/en/activities/diseaseprogrammes/emerging_and_vector_borne_diseases/Pages/EVD-Lab-Net.aspx

[358] http://ecdc.europa.eu/en/aboutus/what-we-do/surveillance/Pages/index.aspx

MediSys (part of the The Health Emergency Operations Facility (HEOF))

The MediSys is a tool developed by the Commission. It collects information from the 'European Media Monitor' in order to improve early detection of bioterrorism activities. By this system, key persons can be alerted about upcoming threats through texts or email. It reinforces the Network for Surveillance of Communicable diseases.[359]

*Health Security Committee (HSC)

The Health Security Committee was set up in 2001 by the EU health ministers and has since then expanded its responsibilities. Among its main tasks are detection and rapid alerts including all types of health threats at the EU level. [360]

EMMa

EMMa is an online mapping tool created by ECDC to support epidemiologists and public health professionals. It aims to facilitate mapping of national and subnational areas worldwide.[361]

The Surveillance Atlas of Infectious Diseases

The Surveillance Atlas of Infectious Diseases is a web-based tool aiming to provide easily available information/data on European infectious diseases and provide good conditions for prevention and control of diseases. It contains diagrams, maps, tables and distributions and users have various search variables such as period or geographical region. [362]

European Influenza Surveillance Network (EISN)

The European Influenza Surveillance Network (EISN) is a European network that monitors influenza (both epidemiological and virological). By providing experts and decision makers with information, the network aims to create better conditions for timely and proper decision making and action. It is coordinated by the ECDC.[363]

[359] http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/medical_intelligence_en.htm

[360] http://ec.europa.eu/health/preparedness_response/risk_management/hsc/index_en.htm

[361] https://emma.ecdc.europa.eu/Pages/home.aspx

[362] http://ecdc.europa.eu/en/data-tools/atlas/Pages/atlas.aspx

[363] http://ecdc.europa.eu/en/healthtopics/influenza/EISN/Pages/index.aspx

Sensemaking

VectorNet

VectorNet launched 2014 as a joint initiative by the European Food Safety Authority (EFSA) and the European Centre for Disease Prevention and Control (ECDC). It is a network for information sharing and data collection on the distribution/ geographical presence of vectors and pathogens in vectors related to health.[364]

*Health Security Committee (HSC)

The HSC works as an information hub in the EU regarding health threats. Besides detection and alerts, it collects data from EU agencies in order to share with member state authorities, provides technical assistance and guidelines to improve national preparedness and can rapidly collect expert opinions during a public health crisis. It promotes connections between alert systems and various actors across sectors. The HSC also develop guidelines and protocols for emergencies, which are tested in exercises.[365]

*RAS CHEM

Besides being a detection and early alert system for chemical incidents, RAS-CHEM operates as a forum of advice and information exchange. The target audience is EU poison centres and Ministries of Health. [366]

*RAS BICHAT

Besides performing detection and rapid alert tasks, Rapid Alert System on Biological and Chemical Attack (RAS-BICHAT) also manage information exchange among partners on suspected or confirmed events. The target audience is members of the Health Security Committee[367]

*Emerging Viral Diseases-Expert Laboratory Network (EVD LabNet)

Besides monitoring and early detection of viral diseases, the EVD LabNet analyses and assesses the treat from identified viral diseases. It provides member states with a common situational picture from a coordinated investigation as well as scientific advice and interpretation. [368]

[364] http://ecdc.europa.eu/en/healthtopics/vectors/VectorNet/Pages/VectorNet.aspx

[365] http://ec.europa.eu/health/preparedness_response/risk_management/hsc/index_en.htm

[366] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf

[367] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf

[368] http://ecdc.europa.eu/en/activities/diseaseprogrammes/emerging_and_vector_borne_diseases/Pages/EVD-Lab-Net.aspx

*The European Surveillance System (TESSy)

TESSy is a database hosted by the ECDC, providing a technical platform for monitoring/surveillance of communicable diseases in Europe. The output from this system is compiled to threat reports published by ECDC. Besides an annual report on epidemiological diseases, several articles and reports are published weekly and monthly on more specified issues. [369]

*HEDIS (part of the The Health Emergency Operations Facility (HEOF))

HEDIS is a web based tool which provides the Commission and the member states with an overview of the situation during a health crisis. It includes sub-portals where relevant information about the threat(s) can be found, including maps, news, scientific advice and a timeline of actions taken. HEDIS also includes forums for information sharing between stakeholders, models for analyzing spread and control of diseases and an interactive disaster analysis system.[370]

*The Epidemic Intelligence Information System (EPIS)

EPIS is a web-based information sharing platform which allows public health experts to exchange information about upcoming and ongoing public health threats. EPIS assesses the possible impact of the identified threats in order to improve coordination of response. All EU member states nominate participating experts to EPIS.[371]

Many EPIS early warning/detection platforms also perform risk assessments, such as;

FWD (Food- and Waterborne Diseases and Zoonoses)

“EPIS-FWD facilitates the early detection and assessment of multi-country/multinational molecular typing clusters and outbreaks of FWDs. The platform connects epidemiologists and microbiologists from 45 countries: 28 EU Member States, three countries of the European Economic Area (EEA) - Iceland, Norway and Liechtenstein - and 14 other non-EU countries”.[372]

STI (Sexually Transmitted Infections)

“EPIS-STI supports the rapid reporting and dissemination of unusual events related to STI transmission across the EU and assess their EU relevance. Reports are submitted by the nominated contact points for STI surveillance in EU/EEA countries. All 31 EU/EEA Member States have access to EPIS-STI”. [373]

[369] http://ecdc.europa.eu/en/aboutus/what-we-do/surveillance/Pages/index.aspx

[370] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf

[371] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx

[372] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx

[373] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx

ELDSNet (European Legionnaires' Disease Surveillance Network)

"EPIS-ELDSNet brings together data on Legionnaires' disease, with a focus on the detection and follow-up of travel-associated clusters, and the investigation of community outbreaks (in an ad hoc fora with restricted access). This allows risk assessment and timely risk communication to the authorities in charge of risk management. "[374]

VPD (Vaccine Preventable Diseases)

EPIS-VPD allows exchange of information on technical topics related to vaccinations and the control of vaccine preventable diseases. The platform connects vaccination programme managers, vaccine experts, epidemiologists and microbiologists from the 31 EU/EEA Member States. [375]

MATRIX

MATRIX is a system which provides member states with assessments on their vulnerability against specific biological and chemical agents. The main target audiences are HSC and EWRS members and committees, and the website furthermore gives access to incident classification tables, guidelines, algorithms for crisis management and health threat focused databases. [376]

*EU Health Security Committee (HSC)

The EU Health Security Committee (HSC) is an advisory group on health security at the European level, including high-level representatives from the Ministries of Health of the EU Member States, Norway, Iceland and Switzerland. The Commission provides the secretariat. European Centre for Disease Prevention and Control (ECDC), European Medicines Agency (EMA) and WHO are observers to the HSC. The HSC provides expertise and has developed member state work plans for threat assessments. The advisory services of HSC can be used for prevention as well as crisis response.[377]

*European Centre of Disease Prevention and Control (ECDC)

Included in the ECDC's mission is to, after identification, assess and communicate current and emerging threats to human health posed by infectious diseases. It aims to pool health expertise and be able to provide advice regarding risks of upcoming and current diseases. [378] Moreover, the centre aims at supporting information sharing among relevant public health actors. [379]

[374] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[375] http://ecdc.europa.eu/en/aboutus/what-we-do/epidemic-intelligence/Pages/EpidemicIntelligence_Tools.aspx
[376] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[377] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf
[378] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf
[379] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf

The EU's Joint Research Centre (JRC) Modeling/Impact Assessment

The EU's Joint Research Centre (JRC) applies mathematical models in order to assess the spread and control as well as effects of health security threat situations such as epidemics. By doing so, they enhance situational awareness and support decision making during a crisis. [380]

Decisionmaking

*The Health Emergency Operations Facility (HEOF) crisis rooms

HEOF was a priority of the Health Security Programme, aiming at setting up a "mechanism for information exchange, consultation and coordination for the handling of health-related issues linked to attacks in which biological and chemical agents might be used or have been used."[381] Included in HEOF is a Crisis room and Communication Centre facility installed in Luxembourg for the management of health security alerts and incidents. This consists of a crisis room, a communication room and one multifunctional meeting room. All operations of the Network for the epidemiological surveillance and control of communicable diseases are conducted from this facility. The HEOF crisis rooms are equipped with various tools for communication during a crisis, such as audio conferencing system for as much as 100 participants and a Digital Alert Communication system.[382]

Coordination

* European Centre of Disease Prevention and Control (ECDC)

In accordance to the Decision from 2013 on on serious cross-border threats to health, the ECDC aims at supporting the EU's preparedness objectives by promoting interoperability among relevant actors. The Centre shall also coordinate the European networking of bodies operating in the fields within the Centres mission and facilitate implementation of joint actions. [383]

*The Early Warning and Response System (EWRS)

During a health crisis such as a pandemic, the Commission leads the EU coordination through the EWRS and keeps in contact with ECDC, WHO, Global Health and Security Initiative (GHSI) and the

[380]http://ec.europa.eu/health/preparedness_response/preparedness/preparedness_planning/index_en.htm#fragment0

[381] http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/heof_en.htm

[382] http://ec.europa.eu/health/preparedness_response/generic_preparedness/planning/heof_en.htm

[383] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf

European Medicines Agency (EMA). In case of a pandemic, the Commission may use a fast track procedure regarding pandemic influenza vaccines.[384]

*Health Security Committee (HSC)

2007 EU health Ministers agreed to extend the HSC mandate to include pandemic preparedness and response as well as coordination of emergency planning at EU level.

According to the Decision from 2013 on serious cross-border threats to health, the Commission and member states shall consult each other within the HSC with a view of coordinating their efforts to develop or maintain capacities to assess and respond to cross border health threats. During crises situations, the HSC ensures coherence of actions by Member States in order to protect human health. [385]

*The Health Emergency Operations Facility (HEOF)

During a health crisis, HEOF ensures coordination between the Commission, Member States, other associated countries and relevant agencies such as European Centre for Disease Prevention and Control (ECDC), European Food Safety Agency (EFSA) and European Agency for the Evaluation of Medicinal Products (EMEA), and international organisations (such as WHO). HEOF also facilitates the decision making process of response measures. [386]

*SANCO public health emergency management

The Health Emergency Operations Facility (HEOF) is a part of SANCO public health emergency management structure, led by a Senior Management Team. This structure activates during a health crisis and stays as long as the "red alert level" is maintained. There are three alert phases; Green – during small sized event, Yellow – during medium or major sized event which can be managed by Health Threats Unit and enhanced operating procedures, Red – during a crisis which cannot be managed by normal procedures. The Senior Management Team is supported by a number of operational teams. All but the communication team is responsible for coordinating actors and response activities. The Emergency Management Team works with the Commissioner and his Cabinet, coordinating the response and establishing policy lines. The External interface coordinates with the Presidency, the Council and the Parliament and, if necessary, the Committee of Regions and Economic and Social Committee. The Internal interface team coordinates activities with different Commission Directorates General and services through ARGUS. The Health Emergency Operations

[384] http://ec.europa.eu/health/preparedness_response/preparedness/preparedness_planning/index_en.htm#fragment1

[385] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf

[386] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf

team contributes to the coordination of health crisis management efforts by the Member States' Ministries of Health, ECDC and International organizations. [387]

European Centre of Disease Prevention and Control Outbreak Assistance Teams

During an outbreak situation, ECDC can mobilize outbreak assistance teams with various disease experts. These teams are permanently available / have a 24/7 readiness to support Member States. The outbreak assistance laboratories network provides microbiology experts. Moreover, ECDC have constant readiness to provide material and administrative support for field missions together with the outbreak assistance teams.[388]

Meaningmaking/Communication

*EU Health Security Committee's Communicators' Network

Recognizing that confusing messages to the public during a crisis can undermine effectiveness of emergency or crisis response, HSC Communicators' network was set up in order to provide reliable and coherent messages to the citizens during a public health crisis. The network discusses communication strategies and conducts meetings in order to better understand the developing situation during a crisis, reviewing media concerns, and discussing public approaches. [389]
HSC Communicators Network supports Member States efforts on risk and crisis communication with the general public during a public health crisis. The HSC also provides a platform for exchange of information between the Member States and the Commission. [390] Continuous contact between communicators within the network supports rapid information exchange during a crisis situation. Information within the network may be shared through the HEDIS (Health Emergency and Disease Information System), and the network has a "Red Book24" which provides information on national communication structures.[391] Globally, the network enables the EU to spread information rapidly worldwide, by connecting with existing communicators' networks under the Global Health Security Initiative and the WHO network under the International Health Regulations (IHR).[392]

*The Health Emergency Operations Facility: Communication

[387] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[388] http://ecdc.europa.eu/en/aboutus/what-we-do/preparedness/Pages/default.aspx
[389] Brussels, 23.11.2009 SEC(2009) 1622 final COMMISSION STAFF WORKING DOCUMENT Health Security in the European Union and Internationally
[390] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf
[391] Brussels, 23.11.2009 SEC(2009) 1622 final COMMISSION STAFF WORKING DOCUMENT Health Security in the European Union and Internationally
[392] http://ec.europa.eu/health/preparedness_response/risk_communication/index_en.htm

The Health Emergency Operations Facility is composed of two teams, one in Luxembourg and the supporting one in Brussels. Besides crisis rooms and meeting rooms, the teams have several communication systems and communication rooms to their disposal. [393]

*SANCO Public Health Emergency Management Structure: Communications Team

The Communication team is one of the operational teams under SANCO public health emergency management structure. The team is in charge of media communication, producing public messages and interaction with other communication officers from member states, relevant organisations and institutions.[394]

Accountability

*EU Health Security Committee (HSC): accountability

The EU Health Security Committee identifies and discusses the lessons learned from past health emergency situations and ensures the follow-up on them. [395]

Reports on the implementation of the legal framework

The Commission is required by law to submit every three years a report on the implementation of the latest legislation which governs the capacities as described above. The reports include an assessment of the operation of the EWRS and of the epidemiological surveillance network, as well as information on how the mechanisms and structures established complement other alert systems.

[393] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[394] http://ec.europa.eu/health/ph_threats/com/preparedness/docs/HEOF_en.pdf
[395] http://ec.europa.eu/health/preparedness_response/docs/hsc_factsheet_en.pdf

The Migration Sector

Introduction

General background

The policy area of migration has a long history within the EU and is closely connected to issues of asylum, free movement of people and external affairs. These issues has historically been handled, primarily by the European Commission (the Commission), and foremost by DG Home and Migration and former DG Relex. However, since the founding of the European External Action Service (EEAS) in 2010 and the establishment of FRONTEX in 26 October 2004 capacitates to handle the ay to implementation of common European migration objectives been moving out of the Commissions institutional framework. Further, migration is not an isolated policy area; there are several overlaps between such as civil protection and counter terrorism. It shall also be mentioned that this inventory is written under the ongoing refugee crisis that has been ongoing since 2015, which makes the line between general capacities and crisis capacities somewhat blurry.

Institutional Landscape

The majority of capacities identified in the migration field are located within the institutional framework of the Commission (primarily in Directorate General (DG) Migration and Home affairs) and the Commission agency Frontex. Further, the DG ofCivil Protection and the European External Action Service (EEAS) is worth mentioning in the context of migration policy relevant EU-departments.

Migration and Home affairs

DG Migration and Home Affairs implement EU-level legislation and rules in the policy areas dealing with cross-border issues, such as asylum, migration, border control, organized crime and terrorism.[396]Furthermore, DG Migration and Home Affair is responsible for the EUs overarching migration policy. The migration area is not one clear cut policy area; DG Migration and Home affairs handles a wide range of migration related policies and agenda setting activities including the implementation of the Schengen agreement, the strive for a common European asylum system and irregular migration.[397] At the time of writing DG Migration and Home affairs Director General is Mr. Matthias Ruete. The premises of DG Migration and Home Affairs are located in Brussels. The organization consists of five main departments dealing with “Strategy and General Affairs”,” Migration and Mobility”, “Migration and Protection”, “Security” and “Migration and Security Funds”.

[396] http://ec.europa.eu/dgs/home-affairs/who-we-are/index_en.htm

[397] http://ec.europa.eu/dgs/home-affairs/index_en.htm

On the political level of the Commission the policy area of migration is currently under the leadership of the Commissioner for migration and Home affairs, Dimitris Avramopoulos.

Frontex

Frontex[398] in its contemporary form was established in 2007[399] and is the European Union's external borderagency. Frontex missions cover a wide range of crisis management tasks related to the management of the external borders of the European Union, for example, Frontex plans, coordinates, implements and evaluates joint operations conducted using Member States' staff. Furthermore, Frontex is involved of the preparation phase of the crisis management by its responsibility to develop common standards for training. Moreover, Frontex serve as an important agency in the process of the detection of potential crisis situations. The agency is responsible for the gathering and analyzing intelligence on the ongoing situation at the external borders. This by gathering data from border crossing points, operational information, information exchange with the member states and open sources. Frontex is also active in the risk assessment covering short- medium- and long-term trends. For this, Frontex monitors the global security environment, political, economic, social, technological, legal and environmental factors that have a possible affect upon the border security of the European Union. [400] The current executive director of Frontex is Mr. Fabrice Leggeri and its premises is located in Warsaw, Poland.

The European External Action Service (EEAS)

At a first glance the involvement of EEAS in the field of migration policy is not self-evident, however the external and the internal dimensions of the EU is not always given. Migration is a policy area connected to global patterns of mobility, to that end migration (and management of migration flows) cannot be reduced to an issue of internal EU affairs. The EU is also working with external actors and third countries in order to manage the ongoing migration crisis. For instance, EEAS handles the partnership agreements with neighboring countries, which includes agreements with third countries on migration and asylum related topicsissues such as migration.[401] The EEAS is located in Brussels, Belgium, and is under the political leadership of Federica Mogherini.

Humanitarian aid, Crisis mangement and Civil Protection

The commissioner responsible for issues of Humanitarian Aid and Crisis Management is Christos Stylianides. As mentioned in previous inventories this organizational design, where one Commissioner

[398] http://Frontex.europa.eu/about-Frontex/origin/
[399] (EC) 2007/2004.
[400] http://frontex.europa.eu/about-frontex/mission-and-tasks/
[401] http://eeas.europa.eu/topics/migration-partnership/408/migration-partnerships_en

is responsible for “Crisis management” , naturally centralizes some of the crisis management capacities worth mentioning in the context of Migration within DG humanitarian aid and Civil Protection. Further, DG humanitarian aid and Civil Protection is worth mentioning in the context of migration funding of one more reason; it supplies economic aid to member states most affected by the refugee crisis.[402]

Inventory

Detection

Coordination Points

Thus few initiatives in the area of detection on record the 2011 project “Coordination Points” is worth Highlighting. Participating in the project were Austria, Poland and Romania and the project recived 40 000 Euro in founding’s from Frontex.[403] The project aimed at improving the exchange of information with the border authorities of Moldova and Ukraine and to work for the establishment of an early warning system of global migration trends.[404]

*Frontex Situation Centre (FSC)

The Frontex Situation Centre (FSC) provides, and continuously update of Europe’s external borders and migration situation. But the FSC has more than an information-gathering function. It acts as a central point of contact and information access for all Frontex stakeholders. The center assist in the area of detection. It provides media monitoring by scanning of big data. Further, FSC works with situational monitoring, providing early alerts an sitiuational pictures to both internal and external clients. Lastly, the FSC offers support to joint operations in the shape of data processing and information sharing structures.[405]

Sensemaking

The Smart Border-package

The "Smart Borders" Package was proposed by the Commission in February 2013.Since then the design and implementation of the proposal has toughly examined in numerous reports (See for example; Technical Study, the executive summary[406], Costs Study[407] and the executive summary of the

[402] http://ec.europa.eu/echo/refugee-crisis_en
[403] http://Frontex.europa.eu/operations/archive-of-operations/E0MVZZ?slug=coordination-points
[404] http://Frontex.europa.eu/operations/archive-of-operations/E0MVZZ?slug=coordination-points
[405] http://Frontex.europa.eu/intelligence/information-management/
[406] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_executive_summary_en.pdf
[407] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf

Impact Assessment[408] The aim of the project is two folded; 1.) To improve the management of the external borders of the Schengen Member States, and 2.) to continue the fight against irregular immigration. Further, the smart boarder-package shall provide information on people who overstay their permits within EU territory, as well as facilitate border crossings for pre-vetted frequent third country national travelers.[409] Thereby, this initiative is geared toward improving the sense making capability among EU personal and will result in a capacity in the Commissions and Frontex toolbox managing extraordinary migration flows.

Visa Information System (VIS)

The Visa Information System (VIS) is a system for information exchange in-between the Schengen states.[410] The design of the system is centered on two main functions; First, there is a central IT system and of a communication infrastructure, Second, there is from the central system connecting this central system to national systems.[411] VIS connects consulates in non-EU countries and all external border crossing points of Schengen States, offering a structure information sharing. Further, it processes data and decisions for applicants that request a short-stay visa to visit the EU or plan to transit within the Shengen area.[412] To the last, the system can perform biometric matching, primarily of fingerprints, for identification and verification purposes.

Risk analysis

Frontex manage issues of risk analysis and assessment related to migration flowss. Frontex collects data from Member States, EU bodies, its partner countries, organizations and from open sources on the situation at and beyond of Europe's borders. The aim of the data collection is to create a picture of the situation at the EU's external borders. Further Frontex risk analysis aims at identifying the key factors that influence the situation at the EUs borders.[413] Further, beyond mapping trends and identifying risks, Frontex provides advice on appropriate operational responses to various challenges. This includes not only migration related risks; it also includes cross-border crime in the areas of EUs external borders. Moreover, Frontex risk analysis is used to advise decision-making within concerned bodies of the EU apparatus as well as used in the daily coordination of joint operations carried out by Frontex.[414] There are three categories of risk analysis carried out by Frontex; 1.) strategic analysis, 2.)

[408] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/securing-eu-borders/legal-documents/docs/20160406/smart_borders_package_-_20160406_-_impact_assessment_-_summary_en.pdf
[409] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm
[410] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm
[411] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm
[412] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/visa-information-system/index_en.htm
[413] http://Frontex.europa.eu/intelligence/risk-analysis/
[414] http://Frontex.europa.eu/intelligence/risk-analysis/

operational analysis and 3.) analytics.[415] Moreover, Frontex carries out a annual risk analysis which is used as a decision basis within the organization.[416]

Schengen information System (SIS II)

The Schengen Information System (SIS) is a large-scale information system that supports external border control and law enforcement cooperation in the Schengen area.[417] The SIS enables authorities, such as police and border guards," to enter and consult alerts on certain categories of wanted or missing persons and objects"[418]. Thus, SIS II serves multiple functions it constitutes a capacity in the field of migration crisis management due to Regulation (EC) No 1987/2006 that regulates border control cooperation. In accordance with the regulation border control cooperation within the EU the SIS-system enables border guards and migration authorities in members tates to check alerts on third-country nationals, which help refusing unwanted individuals entry into or stay in the Schengen Area.[419]

EUROSUR

Eurosur is an additional information sharing system. It is designed improve the management of Europe's external borders. It is located within the institutional framework of FRONTEX and aims to support inMember States by increasing their situational awareness and reaction capability in combating tackling irregular migration and preventing loss of migrant lives at sea.[420] To that end, Eurosor is a sensemaking-capacity in the EU with the purpose of supplying relevant authorities wit relevant information to prevent disasters at sea and tackling illegal immigration at its borders.

EURODAC

The EURODAC Regulation[421] establishes an EU asylum fingerprint database which has been in operation since the year of 2003. The main function of the database is to that when someone applies for asylum, no matter where they are in the EU, their fingerprints are transmitted to the central system of EURODAC.[422] However, this system is not spelled out as a "crisis capacity", however, EURODAC

[415] http://Frontex.europa.eu/intelligence/risk-analysis/
[416] http://Frontex.europa.eu/operations/roles-and-responsibilities/
[417] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm
[418] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm
[419] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm
[420] http://Frontex.europa.eu/intelligence/eurosur/
[421] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm
[422] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/identification-of-applicants/index_en.htm

is a tool for EU-level response, sensemaking and management of asylum seekers and guides collective action.

Automated Border Control (ABC) systems

Automated border control is systems developed within the Frontex framework of border checks. According to the Frontex guide, "Best Practice Operational Guidelines for Automated Border Control (ABC) Systems"[423] , the ABC is "An automated system which authenticates the e MRTD, establishes that the passenger is the rightful holder of the document, queries border control records and automatically determines eligibility for border crossing according to pre-defined rules"[424]. These systems are used for biometric verification and/or identification solutions. Further, Frontex has, in recent times, invested in helping the end-users of these systems in order to handle tradeoffs in-between passenger facilitation and security.[425]

Decisionmaking

In this section we deal with crisis capacities that in different ways offer a institutional framework for crisis induced decision making or actual places made for crisis decision making (e.g crisisrooms). However, the latter category of decision making capacities has not been found in this inventory.

The Temporary Protection Directive

In 2001 athe "Temporary protection directive" was formally adopted by EU authorities, this as a response to the recent conflict in former Yugoslavia and the refugees from the region entering the EU.[426] The directive is a crisis measure geared towards situations of mass influx of refugees and offers a decision making structure to deviate from common regulation in events of crisis. "*The existence of a mass influx of displaced persons should be established by a Council Decision, which should be binding in all Member States in relation to the displaced persons to whom the Decision applies. The conditions for the expiry of the Decision should also be established*"[427]. The directive offers the legal basis to an exceptional measure to provide displaced persons from non-EU countries and unable to return to their country of origin, with immediate and temporary protection.[428] It applies in situations when there is a risk that the standard asylum process in the member states, most affected by the mass influx, struggles to cope with increasing demand evoked by mass influx of refugees.[429] Moreover, the directive is geared to handle situations where there are risks that asylum applicants runs the risk of

[423]http://Frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf
[424]http://Frontex.europa.eu/assets/Publications/Research/Best_Practice_Operational_Guidelines_for_Automated_Border_Control.pdf
[425] http://Frontex.europa.eu/research/border-checks/
[426] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:212:0012:0023:EN:PDF
[427] http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2001:212:0012:0023:EN:PDF
[428] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/temporary-protection/index_en.htm
[429] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/temporary-protection/index_en.htm

negative impact on the processing of claims due to the mounting pressure in the asylum system.[430] Beyond defining a decision making process for trigger and extend temporary protection it foresees harmonized systems for the individuals covered by the measures of temporary protection.[431]

*Rapid-intervention teams

The deployment process of Rapid-intervention teams is discussed in greater detail in the section for "coordination-capacity". However it shall be mentioned that the deployment structure itself constitutes a crisis structure for decision making with pre-established steps an procedures enabling the coordination of national resources. [432]

EU Civil Protection Mechanism

The EU Civil protection mechanism was established in 2001 and is primarily a capacity in terms of civilian protection.[433] The mechanism is located within the institutional framework of DG Humanitarian aid and civilian protection.[434] However, as noted in the above standing section the policy area of migration overlaps with other policy areas. Under large influxes of refuges and other migrants civil protection and migration is intuitively interconnected. By this mechanism of pooled resources of governmental aid the mechanism is an important response-capacity in the immediate aftermath of a disaster or humanitarian crisis. The response can take different forms; "Deployment of specially-equipped teams, or assessment and coordination by experts sent to the field"[435]. Moreover, in the recent refuge crisis the Commission has (via The Civilian Protection Mecanism) coordinated the delivery of immediate material to support Member States and neighbouring countries facing major peaks in the refugees that overwhelmed their immediate response capacities.[436] Thus, it shall be noted the participating and support by the mechanism is voluntary.[437] The Mechanism is coordinated by the European Commission's Emergency Response Coordination Centre (ERCC), "*which is closely monitoring the refugee crisis and facilitates a coherent and efficient European response*".[438] To that end the civilian protection mechanism serve as a capacity in crisis response when

[430] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/temporary-protection/index_en.htm
[431] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/asylum/temporary-protection/index_en.htm
[432] http://frontex.europa.eu/operations/rapid-intervention/
[433] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
[434] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
[435] http://ec.europa.eu/echo/what/civil-protection/mechanism_en
[436] http://ec.europa.eu/echo/refugee-crisis_en
[437] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.320.01.0001.01.ENG
[438] http://ec.europa.eu/echo/refugee-crisis_en

High-Level Dialogues on Migration and third country partnerships

A further important decision making capacity in the field of migration is partnerships with third countries on migration.[439] Since 2015 the EEAS and The commission has been involved in at least 16 dialogues with third countries resulting in partnership agreements involving policy goals related to migration flows.[440] EUs decision making capacity in the making of Partnerships deals with neighboring countries has shown to be an important resource in the light of the increased migration flows both during the Arab spring and the current migration crisis. The EU-Turkey agreement is the most well-known example. In the agreement EU and Turkey aimed to end the irregular migration from Turkey to the EU, and that the EU should offer significant economic support to Turkey in order for Turkey to manage the Syrian refugees within the countries boarders.[441]

Coordination

*Rapid-intervention teams

The rapid intervention teams where established in order to bring assistance to a Member State that is under urgent and exceptional pressure of large number of third-country nationals trying to enter the territory illegally.[442] The operations are organized and planed by FRONTEX: The process of the deployment of rapid intervention teams includes the following steps:

- Request of a Member State to Frontex.
- Information about the request from the Executive Director to the Management Board in Frontex.
- Assessment of the situation based on Frontex risk analysis and information provided by a Member State. The Executive Director may also send experts to the area in order to assess the situation on the spot. (See the section on FSC)
- Decision of the Executive Director of Frontex (no later than five working days from the date of receipt of the request).
- Communication on the decision to the requesting Member State and the Management Board.

[439] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160607/communication_external_aspects_eam_towards_new_migration_ompact_en.pdf
[440] http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160607/communication_external_aspects_eam_towards_new_migration_ompact_annex_2_en.pdf;; http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/european-agenda-migration/proposal-implementation-package/docs/20160607/communication_external_aspects_eam_towards_new_migration_ompact_en.pdf
[441] http://www.consilium.europa.eu/en/press/press-releases/2016/03/18-eu-turkey-statement/
[442] http://Frontex.europa.eu/operations/rapid-intervention/

- If the decision is positive: A.) Preparation of the operational plan (no later than five working days from the date of the decision). B.)Selection and composition of the teams to be sent C.(Deployment (no later than five working days after the operational plan is agreed between the Executive Director and the requesting Member State).[443]

These steps touch upon several of the crisis task examined in the inventories. Including both sense-making activities, a structure for decision making and an effort to coordinate resources.

European Response Coordination Centre (ERCC)

The Emergency Response Coordination Centre (ERCC) is operating within DG ECHO and is connected to the EU Civil Protection Mechanism. ERCC is a "coordination hub" the was set up to support and coordinate a response to disasters both inside and outside European territory.[444] Furthermore, it is worth noting that The ERCC replaces the functions of the previously carried out within the framework of "Monitoring and Information Centre" (MIC). [445] Further; the ERCC supports a range of prevention and preparedness activities, ranging for awareness-raising to field exercises simulating emergency response. In the ongoing, global, refuge crisis the ERCC plays a role by "closely monitoring the refugee crisis and facilitates a coherent and efficient European response".[446]

National Training Coordinators (NTC) Network

Furthermore, Frontex also manages crisis prevention capacities related to coordination in-between relevant Member Sates representatives in the field of training. The NTC Network (NTC) provides Frontex counterparts with a formal platform for continuous dialogue on training matters. Via this platform Frontex aim to promote "a long-term sustainable cooperation with the key actors of border guard agencies".[447]

European Border Guard Teams (EBGT)

The European Border Guard Teams (EBGT) is involved in a wide range of activities. Its activities is located within the institutional framework of Frontex and it fulfills an important capacity in the field of migration management. It is relevant as a capacity for the management of sharp rises in migration for two main reasons. First, because of its function when it commes to assisting in the process of identifying nationalities of irregular migrants detected at the borders. Furthermore and second, the EBGT provides training of national personal.[448] To that end, EBGT is a coordinating capacity in the category of crisis preparation activities..

[443] http://Frontex.europa.eu/operations/rapid-intervention/
[444] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[445] http://ec.europa.eu/echo/what/civil-protection/emergency-response-coordination-centre-ercc_en
[446] http://ec.europa.eu/echo/refugee-crisis_en
[447] http://Frontex.europa.eu/training/training-infrastructures-and-networks/
[448] http://frontex.europa.eu/operations/european-border-guard-teams/

The EBGT and its mission were established in the new Frontex regulation that came into force in December 2011. The document specifies the conditions for deployment in Frontex joint operations and rapid border interventions.[449] The EBGT is composed by a range of personnel spanning from border guards supplied by the EU Member States, experts in different areas of border management including land and sea border surveillance. For instance they train personnel in order teach them how to debrief migrants in a way which enables the systematic extraction of information for intelligence purposes from migrants willing to cooperate.[450] Other examples of training performed by EBGT includes how to deal with the assumption of nationality and identity among undocumented migrants, how to identify vulnerable persons during a screening interview, basic fact finding interviews in migrant interviews and techniques for examination of all kinds of border-related documents.[451]

EBGT consists of personal supplied by the Member States. This pool of personal is recruited based on specific expert profiles. Following the selection process Frontex provides training of team members, relevant to their field of expertise, and the tasks that they performed. All members of EGBT will receive training in relevant union and international law, including fundamental rights and access to international protection.

Joint operations

Joint operations is an example of EUs skill when it comes to institutionalizing procedures for coordination of pooled resources from the member states. Frontex is also organizing joint operations upon requests from Member States. This capacity The Joint operations performed by Frontex are planned and developed on the basis of an Annual Risk Analysis Report.[452] The risk analyses describe the likely future risk of irregular migration along the EU external border (See section "risk analysis"). During the annual meetings with Member States the agency then prioritizes the proposed joint operations on the basis of their importance and the resources available in order to ensure an effective response.[453] Moreover, Frontex plans the operations together with the host country whom requested the operation. Thereinafter, they proceed by an assessment of the number of officers needed to carry out the mission and evaluate the need for specific expertise, consider the quantity and type of technical equipment required to fulfill the proposed mission.[454] Furthermore, joint operations include operational planning and implementation of the mission. During the operation the deployed guest officers work under the command of the authorities of the host country. Moreover, the joint operations

[449] http://frontex.europa.eu/operations/european-border-guard-teams/
[450] http://Frontex.europa.eu/training/ebgt-training/
[451] http://Frontex.europa.eu/training/ebgt-training/
[452] http://Frontex.europa.eu/operations/roles-and-responsibilities/
[453] http://Frontex.europa.eu/operations/roles-and-responsibilities/
[454]http://Frontex.europa.eu/operations/roles-and-responsibilities/

are ruled by a common code of conduct and evaluations of the missions are performed by Frontex personnel.[455]

Partnership Academies (PA) Network

The Partnership Academies network constitutes what is described as “a key element” in promoting excellence in border guard education and training by maintaining cooperation with European law enforcement stakeholders.[456] This network of national border guard academies supports Frontex by hosting training activities and by promoting the share of expertise in education and training projects. The network contributes to enhanced cooperation, common use of resources and ensures quality of professional performance in Europe and beyond.[457]

Meaningmaking/Communication

The inventory of the migration policy area hasn’t revealed any EU specific capacities for communication or meaning making (e.g official crisis communication plans or procedure). However, existing venues such as twitter, former commissioner of Home affairs, Cecilia Malmströms blog and webpages on the ongoing refugee crisis frequently approach issues of migration and refugees.

Twitter

Twitter is frequently used by several EU institutions in a way that touch upon issues and turns in migration flows. For example the current Commissioner for Migration and Home affarirs, Dimitris Avramopoulos, twitter account [458]does, on a daily basis, approach the ongoing European migration crisis. Further, the European Parliament[459], EEAS[460] and DG Migration and Home affairs[461] are active on twitter and with the current focus in the public debate on migration; social media seems to be crisis communication capacities worth highlighting.

Webpage: Refugee crisis in Europe

The European commission has set up a temporary webpage on the ongoing refugee crisis and the measurements taken by the EU and the European Commission to handle the situation.[462] The homepage is administrated by DG Humanitarian aid and civil protection. [463]

[455] http://Frontex.europa.eu/operations/roles-and-responsibilities/
[456] http://Frontex.europa.eu/training/training-infrastructures-and-networks/
[457] http://Frontex.europa.eu/training/training-infrastructures-and-networks/
[458] https://twitter.com/Avramopoulos
[459] https://twitter.com/europarl_en
[460] https://twitter.com/eu_eeas
[461] https://twitter.com/euhomeaffairs
[462] http://ec.europa.eu/echo/refugee-crisis_en
[463] http://ec.europa.eu/echo/refugee-crisis_en

Webpage: Timeline - response to migratory pressures

This webpage is provided by European Council Council of the European Union and offers a timeline of events "On how the crisis unfolded in 2015, and how the EU developed its comprehensive response. It covers 9 months of crisis in 2015, as told by key witnesses from the Council of the EU and the European Commission"[464]. To that end the webpage is a capacity designed to communicate the EU response to the citizens of the EU.

Accountability

So what is an accountability capacity in the field of migration? In this section there are a number of funds established within the European Union framework that in different ways are designed to, in different ways, ease the effects of extreme influxes of third countries nationals due to effects of transnational crisis for the effected member states. In this section we deal with capacities gered towards recovery and restored public confidence.

External Borders Fund (EBF)

Was a fund active during the year of 2007, the fund was designed to provide financial support to assist member states in responding to large influx of migrants. Furthermore, the fund has financed a large number of projects, especially in member states located in geographically exposed to a large number of migrants. The EIF aims at, by supporting countries most exposed for migration pressure, to improve the implementation of common standards for control of the EU's external borders.[465] represents a heavy burden. Further, the Fund also supports actions for managing efficient controls. [466]

European Fund for the Integration of third-country nationals (EIF)

EIF was established in order to facilitate integration. Furthermore, and the Union for managing effectively security-related risk and crisis, and preparing for protecting people and critical infrastructure against terrorist attacks and other security related incidents.[467] By striving for fast integration on newly arrived migrants and refugees this fund is labeled as a accountability capacity that aims to restoring public confidence in current crisis situation.[468]

The Asylum, Migration and Integration Fund

The "Asylum, Migration and Integration Fund" (AMIF) areis a fund with the recources of 3.137 billion Euros. the fund is aimed at promoting efficient management of migration flows and the

[464] http://www.consilium.europa.eu/en/policies/migratory-pressures/history-migratory-pressures/

[465] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/external-borders-fund/index_en.htm

[466] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/external-borders-fund/index_en.htm

[467] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/integration-fund/index_en.htm

[468] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/integration-fund/index_en.htm

implementation, strengthening and development of a common Union approach to asylum and immigration.[469] The fund will be active for seven years (2014-2020) and is a capacity to restore accountability and handling the aftermath of the refugee crisis. This Fund will contribute to the achievement of four specific objectives.[470]

Research, Frontex

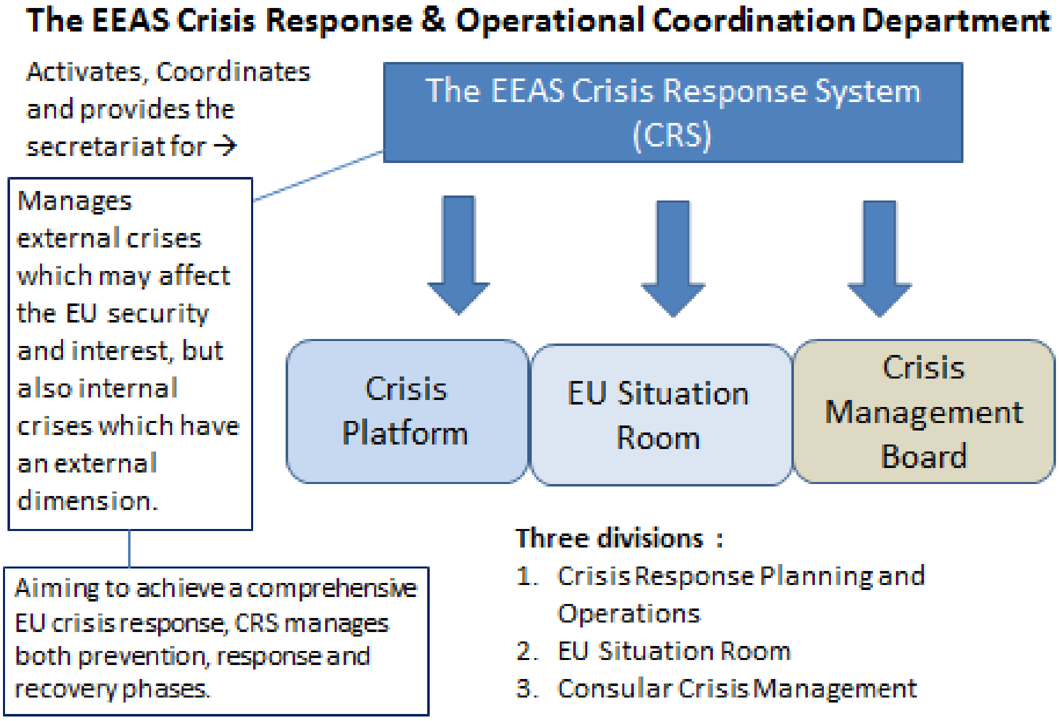
Frontex conduct research in numerous areas. As a capacity this foremost is concentrated on issues closely linked to crisis preparation and prevention. However, Frontex research program is geared towards numerous issues such as advanced technologies and Technical assistance to the European Commission, Member States and Third Countries etc.[471]

[469] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/asylum-migration-integration-fund/index_en.htm

[470] http://ec.europa.eu/dgs/home-affairs/financing/fundings/migration-asylum-borders/asylum-migration-integration-fund/index_en.htm

[471] http://Frontex.europa.eu/research/role/

Part II: Council of Ministers of the European Union/ European Council Crisis Management Capacities


The EEAS Crisis Response & Operational Coordination Department
Activates, Coordinates and provides the secretariat for →
The EEAS Crisis Response System (CRS)
Manages external crises which may affect the EU security and interest, but also internal crises which have an external dimension.
Crisis Platform
EU Situation Room
Crisis Management Board
Aiming to achieve a comprehensive EU crisis response, CRS manages both prevention, response and recovery phases.
Three divisions :
1. Crisis Response Planning and Operations
2. EU Situation Room
3. Consular Crisis Management

Detection

The Crisis Response Planning and Operations-division of the EEAS Crisis Response & Operational Coordination Department

- The "Crisis Response Planning and Operations"-division of the department closely monitors potential crises in the world in order to enable a fast response.[472]

Sensemaking

The Crisis Response Planning and Operations-division of the EEAS Crisis Response & Operational Coordination Department

- The "Crisis Response Planning and Operations"-division has responsibility for overall planning of crisis management activities. [473]

[472] http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm
[473] http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm

The EU Situation Room-division of the EEAS Crisis Response & Operational Coordination Department

- The EU Situation Room keeps a 24/7 situational awareness and worldwide crisis monitoring.[474]
- It functions as an information hub for EU institutions and collects crisis information provided from Member States, international organizations and EU delegations and others. The Situation Room is also the contact point for crisis centres of other regional organizations around the world as well as Member States crisis centres. [475]

The integrated crisis response (IPCR): ISAA

- During a crisis, the EEAS and the Commission together form an Integrated Situational Awareness and Analysis (ISAA) which supports the Presidency and the decision making of the Council. [476]

The integrated crisis response (IPCR): IPCR Web-Platform

- The IPCR Web-platform functions as an information sharing tool and a crisis room. It is owned by the Council and allows relevant stakeholders from both Member States and EU-level to timely exchange crisis information which may be used for analysis and decision making. The website may be used both in normal conditions as well as crisis conditions. It can monitor upcoming events which may lead to activation of IPCR. [477]

The integrated crisis response (IPCR): Exercises

- In order to spread the IPCR "culture", exercises and training courses for decision makers are held in order to raise awareness and level of preparedness. [478]

Decisionmaking

The Crisis Platform of the EEAS Crisis Response & Operational Coordination Department

The Crisis Platform is an external crisis mechanism (coordinated by the Crisis Response Planning and Operations division) chaired by the High Representative, the EEAS Executive General (ESG) or the EEAS Managing Director for Crisis Response. It can bring together various military and civilian crisis management actors/structures depending on the crisis in question. It has proved to be an important instrument for external crisis decision making within the EU (for example used in the Libyan crisis and the arab spring).[479]

[474] http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm
[475] http://eeas.europa.eu/crisis-response/what-we-do/eu-situation-room/index_en.htm
[476] Council of the European Union: The EU integrated political crisis response arrangements
[477] Council of the European Union: The EU integrated political crisis response arrangements
[478] Council of the European Union: The EU integrated political crisis response arrangements
[479] http://eeas.europa.eu/crisis-response/what-we-do/crisis-platform/index_en.htm

The integrated crisis response (IPCR): Coordination/Decisionmaking

- In 2013, the EU Integrated Political Crisis Response arrangements (IPCR) replaced the previous EU Emergency and Crisis Coordination Arrangements (CCA), aiming to improve EU-level decision making as well as coordination during major crises. [480]
- The Presidency is in lead, but supported by the General Secretariat of the Council (GSC), the European Commission, the European External Action Service (EEAS) and, in the case of terrorist attacks, the EU Counter-Terrorism coordinator. [481]
- The IPCR allows the Council to coordinate during an invocation of the solidarity clause. [482]
- The IPCR is based on a progressive approach. Its activation by the Presidency, at the request of the affected member state(s), leads to a number of stages, starting from situational awareness to political coordination and decision-making, at Coreper, Council or even European Council level." [483]

Coordination

EEAS Crisis Response & Operational Coordination Department

- Coordinates the mobilization of crisis management measures, including instruments and actors.
- Continues to coordinate and ensure coherence of actions in the following phases of crisis management.
- The department is responsible for the implementation of the comprehensive EU crisis response.

The Crisis Response Planning and Operations-division of the EEAS Crisis Response & Operational Coordination Department

- The "Crisis Response Planning and Operations"-division assists the EU High representative to coordinate crisis management response and coordinated the action of the EU Crisis Platform.

The EU Situation Room-division of the EEAS Crisis Response & Operational Coordination Department

- The situation room supports the EU Integrated Political Crisis Response arrangements (IPCR) and cooperates closely with the Commission to support coordination of complex crises.[484]

[480] Council of the European Union: The EU integrated political crisis response arrangements
[481] Council of the European Union: The EU integrated political crisis response arrangements
[482] Council of the European Union: The EU integrated political crisis response arrangements
[483] Council of the European Union: The EU integrated political crisis response arrangements
[484] http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm

The Consular Crisis Management-division of the EEAS Crisis Response & Operational Coordination Department

- The “Consular Crisis Management”-division functions as a support for a coordinated crisis response. [485] For example, it supports the Presidency to coordinate crisis management. The CoOl (Consular OnLine) provides a website where member states and a few external states (Switzerland, Norway, the US, Canada and Australia) may cooperate during a crisis.[486]

[485] http://eeas.europa.eu/crisis-response/what-we-do/index_en.htm

[486] http://eeas.europa.eu/crisis-response/what-we-do/consular/index_en.htm

Part III: Descriptive Statistics

European Commission Crisis Management Capacities

Sector	*Total number of capacities*
Energy	*30*
Cyber	*25*
Counter Terrorism	*30*
Civil Protection	*23*
Transport	*33*
Health	*45*
Migration	*26*
All sectors	*212*

Tasks	*Total number of capacities*
Detection	46
Sensemaking	75
Decisionmaking	14
Coordination	35
Meaningmaking/Coordination	18
Accountability	24

Figure I

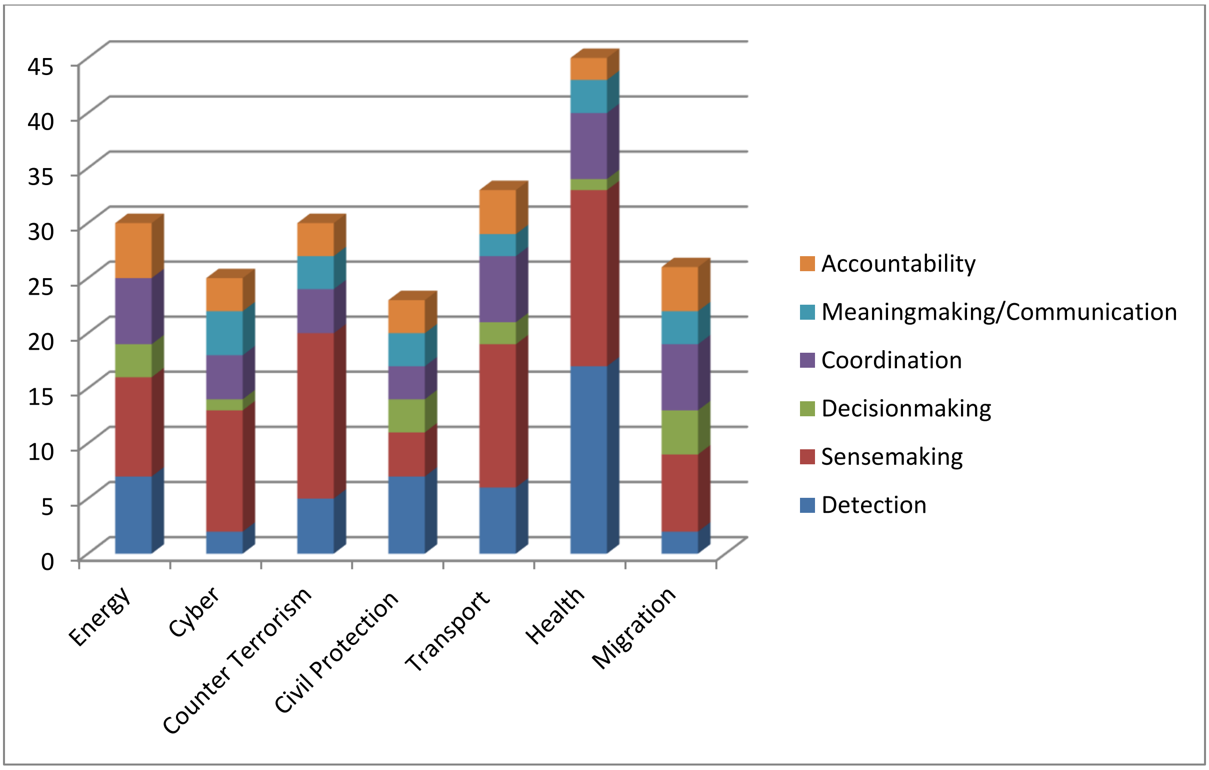


Figure II

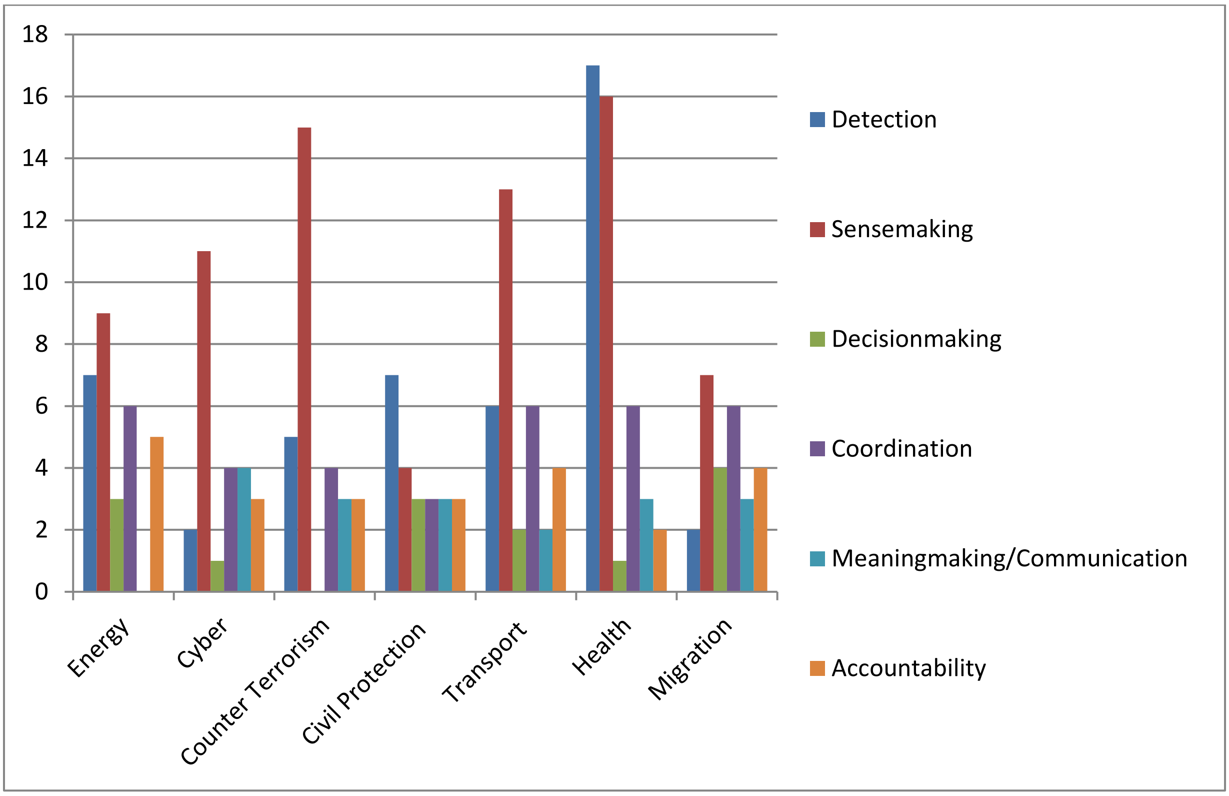
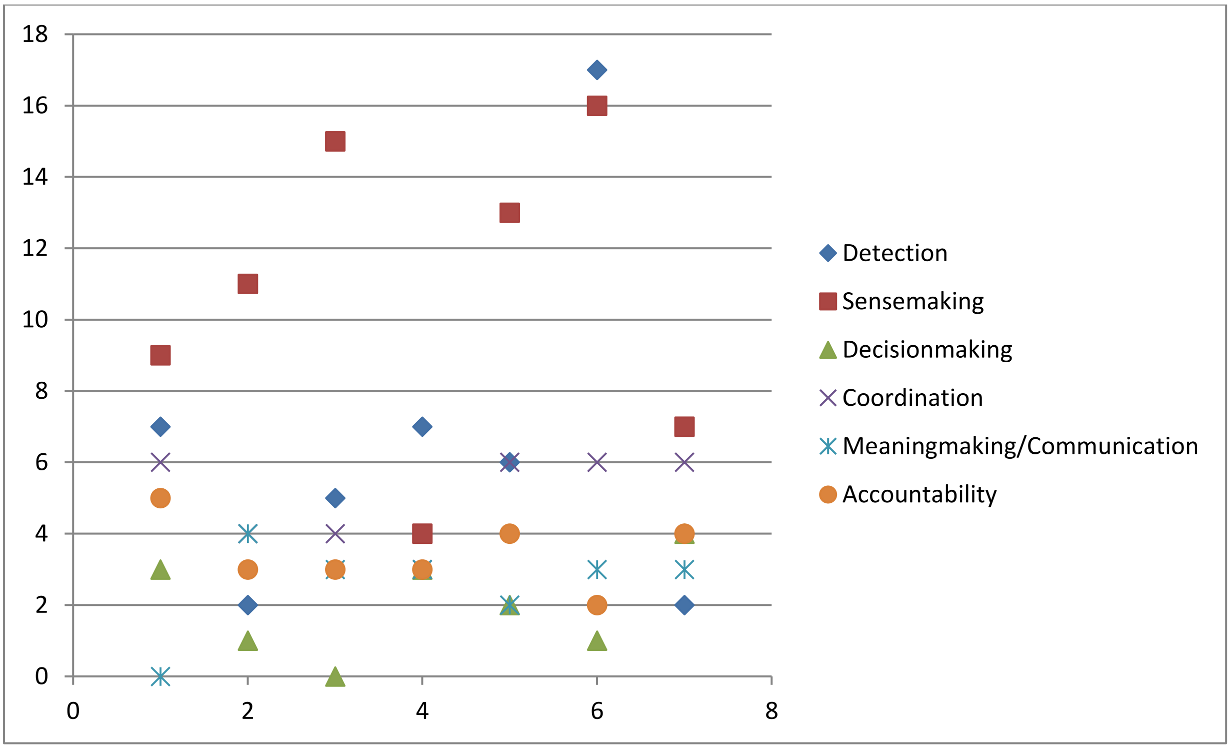


Figure III


Detection
Sensemaking
Decisionmaking
Coordination
Meaningmaking/Communication
Accountability