EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Economic and Monetary Affairs

Employment and Social Affairs

Environment, Public Health and Food Safety

Industry, Research and Energy

Internal Market and Consumer Protection

The role of ENISA in contributing to a coherent and enhanced structure network and information security in the EU and internationally

ITRE

EN

2011

DIRECTORATE GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A: ECONOMIC AND SCIENTIFIC POLICY

INDUSTRY, RESEARCH AND ENERGY

The role of ENISA in contributing to a coherent and enhanced structure of network and information security in the EU and internationally

STUDY

Abstract

This study provides analysis to support an ongoing discussion over the future course of ENISA. It assesses many aspects of the effectiveness of ENISA, and considers possible ways to improve its efficiency and effectiveness going forward. The level and balance of staffing, and the efficiency of mission-related travel arrangements, prove to be important factors.

IP/A/ITRE/ST/2011-04
PE464.432

July 2011
EN

This document was requested by the European Parliament's Committee on Industry, Research and Energy

AUTHOR(S)

Mr J. Scott Marcus
Dr Marieke Klaver
Ms Gabriela Bodea
Ms Annette Hillebrand
Mr Peter Stamm

RESPONSIBLE ADMINISTRATOR

Adél Holdampf
Policy Department Economic and Scientific Policy
European Parliament
B-1047 Brussels
E-mail: Poldep-Economy-Science@europarl.europa.eu

LINGUISTIC VERSIONS

Original: [EN]
Executive Summary: [DE, FR]

ABOUT THE EDITOR

To contact the Policy Department or to subscribe to its monthly newsletter please write to: Poldep-Economy-Science@europarl.europa.eu

Manuscript completed in July 2011.

This document is available on the Internet at:
http://www.europarl.europa.eu/activities/committees/studies.do?language=EN

DISCLAIMER

CONTENTS

LIST OF ABBREVIATIONS

CCD COE	Cooperative Cyber Defence Centre of Excellence (NATO)
CDMA	Cyber Defence Management Authority (NATO)
CEN	European Committee for Standardization (Comité Européen de Normalisation)
CENELEC	European Committee for Electrotechnical Standardization (Comité Européen de Normalisation Électrotechnique)
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIP	Critical Infrastructure Protection
CSOC	Cyber Security Operations Centre (UK)
DAE	Digital Agenda for Europe
ED	Executive Director
EDA	European Defence Agency
EDPS	European Data Protection Supervisor
EFMS	European Forum for Member States
EISAS	European Information Sharing and Alert System
ENISA	European Network and Information Security Agency
EP3R	European Public Private Partnership for Resilience
ETSI	European Telecommunications Standards Institute
EuroSCSIE	European SCADA and Control Systems Information Exchange
ICT	Information and Communication Technologies

ISO	International Organization for Standardization
ISP	Internet Service Provider
ITRE	Industry, Research and Energy
ITU	International Telecommunication Union
MB	Management Board
MFF	Multiannual Financial Framework
MS	Member State
NCIRC	NATO Computer Incident Response Capability (NATO)
NCO	National Contact Officer
NIS	Network and Information Security
NLO	National Liaison Officers
OCS	Office for Cyber Security (UK)
OECD	Organization for Economic Co-operation and Development
PCS	Process Control Systems
PPP	Public Private Partnership
PIA	Privacy Impact Assessment
PSG	Permanent Stakeholders Group
SCADA	Supervisory Control And Data Acquisition
SME	Small and medium-sized enterprises
WPK	Workpackage
WS	Work stream

LIST OF TABLES

LIST OF FIGURES

FOOD FOR THOUGHT

LIST OF RECOMMENDATIONS

LIST OF INTERVIEWEES

We contacted the following interviewees, either for a full interview or for a shorter and more focused discussion.

Prof. Udo HELMBRECHT	ENISA Executive Director
Dr. Steve PURSER	ENISA Head of the Technical Competence Department
Dr. Andreas MITRAKIS	ENISA Head of the Administration Department
Ms. Mari HERRANEN	Chair, ENISA MB
Prof. Reinhard POSCH	ENISA Former Chair, current MB Member (Austria)
Prof. Constantine STEPHANIDIS	ENISA MB Member (Greece), Head of FORTH, Heraklion
Geoff SMITH	ENISA MB Member (UK)
Edgar de Lange	ENISA MB Member (the Netherlands)
Maarten BOTTERMAN	PSG Member, Head of GNKS Consulting
Gabriella CATTANEO	IDC, Research Director, Head of 2007 Evaluation
Fabio COLASANTI	Former Director General, DG INFSO
Silver TAMMIK	Counsellor for Economic Affairs, Estonia[1]
Bernardo CORREIA	ETSI, External Relations, Partnerships and EU Affairs
John KETCHELL	CEN/CENELEC, Director of Innovation
Alain VIALLIX	Alcatel-Lucent expert
Wim HAFKAMP	Rabobank and FI-ISAC, Security Manager

[1] Permanent Representation of Estonia to the EU, Estonian Ministry of Economic Affairs and Communications

EXECUTIVE SUMMARY

Background

ENISA was initially established from 14 March 2004 for a period of five years.[2] The period of establishment was subsequently extended to March 2012,[3] and has just been amended again to extend ENISA's lifetime *à l'identique* until September 2013.[4] In parallel with this, the Commission put forward a legislative proposal in September 2010 to modernise and streamline ENISA,[5] and has accompanied the proposal as required with an impact assessment.[6] The current study must thus be seen in the context of an ongoing discussion over the future course of ENISA.

Which way forward?

In principle, there is always the question: should the agency continue as it is, should it be abolished, or should it be changed going forward? In this case, the answer at this level of discussion seems to be fairly clear.

In the case of ENISA, we think that a widespread consensus has emerged that the agency meets real needs at European level, that it would be challenging and costly to achieve the same ends through interaction among the players at national level, and that an agency such as ENISA is thus the most efficient and appropriate way to achieve the necessary coordination at European level.

It is also fairly clear that continuation of the agency exactly as it is would be inappropriate. First, new challenges and missions for ENISA are emerging all the time, including (1) conducting cyber security exercises at European level and optionally in cooperation with the US; (2) coordinating the reporting of breach notifications, as required in the 2009 modifications to the regulatory framework for electronic communications; and (3) interactions with cybercrime, electronic privacy, and other stakeholders in neighbouring policy domains. Second, ENISA faces multiple well-known challenges to its effectiveness and efficiency, many of which ENISA itself cannot correct.

An evolving mission for ENISA

ENISA was established to deal with Network and Information Security (NIS), which encompasses both cyber security and Critical Information Infrastructure Protection (CIIP). As computing and communications take on ever-increasing significance in the daily lives of Europeans, the risks associated with cyber threats and also with possible critical infrastructure disruption become increasingly worrisome.

---

[2] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Article 27.

[3] Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[4] REGULATION (EU) No 580/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[5] 2010/0275 (COD); Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), COM(2010)521.

[6] SEC(2010) 1126, Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1126:FIN:EN:PDF.

ENISA has always been engaged with a large number of private and governmental Computer Emergency Response Teams (CERTs) around Europe, but over time ENISA's potential and actual mission has broadened and deepened. That threats to cyber security are intensifying over time needs no elaboration. But the number and nature of stakeholders involved with cyber security and CIIP continues to grow over time. At international level, for instance, relevant fora include the G8, OECD, OSCE, NATO, the EU-US working group on cyber security and cybercrime, and the Council of Europe.

The growing number and complexity of these interactions imply a growing need for the kind of capabilities that ENISA is uniquely placed to offer: providing European coordination when needed, and offering a platform for dialogue and a means to exchange best practice for NIS at European level. Conversely, for each national NIS entity to attempt to maintain such a wide web of interactions would be inefficient.

ENISA today

ENISA is doing well today. It is under competent management, its finances are in order, and it has built a respected professional team that is highly qualified in terms of degrees and years of relevant experience.

The work that it does appears to be highly appreciated by its stakeholders. This is also reflected in a steady growth in the tasks that it is asked to take on.

At the same time, ENISA faces a number of challenges to its effectiveness and efficiency, many of which were already known when it was last formally evaluated in 2006-2007. ENISA faced, and continues to face, two significant challenges in regard to efficiency, and these dwarf the others: (1) a small staff size, which inherently implies a relatively high ratio of administrative staff to total staff; and (2) a relatively remote and inaccessible location that implies high travel costs as well as challenges to recruiting and retention. When one considers that ENISA suffers *both* from small size and a remote location, the agency faces among the greatest combined challenges to efficiency of any European decentralised agency.

The 2007 evaluation took place early in ENISA's life, and under a different management team. ENISA has made progress in many areas. As regards the ratio of administrative staff to total staff, for instance, ENISA is now on a par with its peer group of decentralised agencies with fewer than 75 employees. But ENISA is still small, and administrative overhead is still relatively high compared with larger institutions.

The location continues to negatively impact ENISA's ability to conduct missions, which is a serious concern for an agency that exists primarily for purposes of liaison and coordination. The crucial issue with respect to travel is not the travel expenses themselves, but rather the lost time for key knowledge workers, which implies a substantially reduced number of missions per knowledge worker per year.

Whether a new ENISA Regulation leads to a formal change in ENISA's mission or not, its mission has grown and will continue to grow. One example of this is the breach notification responsibilities assigned to ENISA under Articles 13a and 13b of the Framework Directive[7], which may imply a somewhat operational data collection role for ENISA for the first time. Another is the need to conduct exercises (at European level and with third countries including the US). Both are examples of new high value-add activities that have now effectively become part of ENISA's mission.

[7] Directive 2002/21/EC (Framework Directive) as amended by Directive 2009/140/EC (Better Regulation Directive).

ENISA tomorrow?

We considered a wide range of questions about ENISA going forward, including its mission, its budget and staffing, and any measures that might improve efficiency or effectiveness.

We think that ENISA's period of establishment should either be made indefinite, of failing this should be aligned with the Multiannual Financial Framework (MFF) (2014-2020). ENISA has demonstrated its usefulness.

As regards the mission, we think that the 2004 ENISA Regulation largely took the correct approach by crafting a flexible framework, and enabling ENISA management together with the Management Board (MB) and in consultation with the Permanent Stakeholders' Group (PSG), to adjust the ongoing Work Programme to meet changing needs. Some have argued that the current Regulation is ambiguous, a claim which seems to have some validity given that ENISA has been subject to widely divergent expectations from its stakeholders. We think that some re-crafting of the mission is in order so as to reduce ambiguity.

The 2004 Regulation restricts ENISA's ability to interact with cybercrime and with data privacy issues, both of which have points of intersection with NIS. We think that clarifications are in order so as to facilitate ENISA's ability to play a supportive role, but not to duplicate existing capabilities.

There has been a long-standing belief that ENISA does not do operational tasks, and should never take on operational tasks. We think that this view is simplistic. There are different kinds of operational tasks, some of which are appropriate for ENISA to take on, others of which are appropriate only if the benefits are large enough to outweigh the significant costs, and still others of which would probably never be appropriate. The non-real-time handling of data that is sensitive either for security or for privacy reasons is an operational task, but ENISA has already been assigned such a task in regard to security breach notifications. We recognise that ENISA will have to invest effort to prepare itself for this task, but we consider the task to be appropriate. Taking on operational duties that the Member States are already equipped to do is probably never appropriate. But taking on 24 x 7 responsibilities that have no overlap with Member State activities could be appropriate, depending on the balance of benefits to costs.

As regards the level of staffing, we conclude, as the Commission has, that an increase to a staff size of roughly 100 over the period 2012-2016 is in order. Recognising that there are budget constraints, we nonetheless suggest starting the ramp sooner than in the Commission's projections. This reflects the recognition that the workload has been steadily increasing over the past few years, that it will predictably continue to increase over the next few years, and that there are already some areas where ENISA arguably should be doing more if it had the resources.

Any increase in staff should be accompanied by balanced attempts to address long-standing inefficiencies to which ENISA is subject.

The largest single potential efficiency improvement would seek to address the travel inefficiency posed by ENISA's relatively remote location in Heraklion. The opening of a liaison office in Brussels, together with a branch office of modest size in Athens, would appear to represent a simple and cost-effective way to increase the number of missions that can be undertaken on average per knowledge worker per staff year. Just one third of ENISA employees conduct two thirds of all ENISA mission travel, and a large fraction of these trips are to Brussels.

The Brussels liaison office together with a branch office in Athens could also help address long-standing challenges in recruiting and retaining senior staff.

We have studied these issues in detail, and we believe that these are realistic options that could be put in place, under suitable conditions, prior to enactment of a new ENISA Regulation.

We considered a number of additional potential clarifications, organisational changes, and efficiency gains, many of which were already identified in the Commission's proposal. These appear in the report itself.

An impact assessment

The Options in the Commission's impact assessment did not address the issues that in our judgment needed to be addressed, so we included an abbreviated impact assessment in this study. We based our analysis on the following set of Options:

Policy option	Description
OPTION 1: No policy	The ENISA mandate expires; however, other activities at European and Member State level continue without change.
OPTION 2: Business as usual	On 14 March 2012, the mandate of ENISA is further extended. Mission: • To the extent that ENISA's mission has already expanded, those changes carry forward. • To the extent that ENISA's mission would likely expand within the scope of the current Regulation, those changes are also reflected. Only small increases in staff are assumed. Only small increases in efficiency are assumed.
OPTION 3a: Same mission, enhanced resources	Same mission as in OPTION 2. Increase in staff size begins in 2012.
OPTION 3b: Same mission, enhanced resources and efficiency	Same mission as in OPTION 2. Increase in staff size begins in 2012, but more slowly than in OPTION 3a. Emphasis on increased staff efficiency, especially as regards travel and recruitment. A Brussels liaison office and a small branch office in Athens are assumed.
OPTION 4: Add a CERT for EU institutions to ENISA's mission.	Same mission as in OPTION 2, plus a CERT for the EU institutions. Staff needs to expand to enable an operational 7x24 role, and an expanded Brussels liaison office. This Option assumes the same efficiency gains as in Option 3b, and staff growth for functions other than the CERT that is also in line with Option 3b.

Working with these Options enabled us to focus on different staff increase ramps, and on the effects of a Brussels liaison office and a branch office in Athens. As previously noted,

we see benefits in a balanced approach that seeks both staff size increase and gains in effectiveness and efficiency.

Option 1 (no policy and thus no programme) is lowest cost, but is ineffective – the problems that ENISA was created to address would remain, and other institutions would not fill the gap. Option 2 (business as usual) does not provide capacity for growth, and would likely result in inability to accomplish parts of ENISA's current mission inasmuch as the new tasks that would compete for the same resources that are now serving current tasks. Options 3a (more resources) and 3b (a blend of increased resources and efficiency gains, especially as regards travel) provide the needed capacity. Option 3b would appear to be superior to the others in terms of efficiency and effectiveness, and superior to 3a in terms of direct cost.

As a more radical option, we also considered having ENISA take the lead in running a CERT for the European institutions. This implies a 24 x 7 role for ENISA, but for reasons previously noted we think that it is not unrealistic. There are numerous considerations that would have to be weighed against any benefits. The creation of a pre-configuration team for this CERT was publicly announced just a few days ago, on 10 June 2011.[8] The pre-configuration team is supposed to spend the next year planning for possible implementation of such a CERT. Thus, there are a great many unknowns. For now, however, this Option serves as a plausible illustration of one possible evolutionary direction for ENISA.

[8] Cyber security: EU prepares to set up Computer Emergency Response Team for EU Institutions, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694.

1. INTRODUCTION

The European Parliament's Committee on the Industry, Research and Energy (ITRE) has requested a research study to "address the tasks of ENISA with a view towards ensuring that ENISA can contribute effectively to a coherent and enhanced structure for network and information security in the EU and internationally, including in relation to interacting with national CERTs, while respecting Member States' internal organisation of their network and information security activities and taking into consideration the activities of other bodies (whether EU or not) active in the field of cyber security." As required under our terms of reference, we have considered "all practical arrangements, including human resource issues, conducive to the effective performance by ENISA of its tasks, as well as budgetary aspects necessary for ENISA to adequately fulfil its role."

This brief introduction discusses our methodology for this report at length. We then provide a quick overview of possible ways forward for ENISA, a topic that is taken up in far greater detail in Section 4 of this report. We note the role of ENISA's location in the discussion, and then present the overall structure of this report.

ENISA was initially established from 14 March 2004 for a period of five years.[9] The period of establishment was subsequently extended to 2012,[10] and has just been amended again to extend ENISA's lifetime *à l'identique* until 13 September 2013 to permit time for discussion of the future course of ENISA.[11] In parallel with this, the Commission put forward a legislative proposal in September 2010 to modernise and streamline ENISA. [12] The current study must thus be seen in the context of an ongoing discussion over the future course of ENISA.

1.1. Our methodology

Our initial intent was to use a conventional approach to the study: (1) conducting general desk research, (2) drawing on the evaluation conducted in 2007 and the Commission's summaries of the two consultations that they conducted, (3) factoring in the results of the Commission's 2010 proposal and especially of the associated impact assessment document, (4) supplementing these sources with interviews, (5) comparing and assessing the results to arrive at findings, and (6) arriving at a set of recommendations.

In the event, this approach would not have been sufficient. Our initial examination of the relevant documents raised questions about the objectivity, completeness, methodological suitability, and/or reliability of many of the documents on which we normally would have relied. We found it necessary to do a much more critical and comprehensive analysis than should have been needed. In particular, we had to determine which documents we could rely on, and which should be taken with a grain of salt.

[9] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Article 27.

[10] Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[11] REGULATION (EU) No 580/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[12] 2010/0275 (COD); Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), COM(2010)521.

A notable exception to all of this is the 2007 evaluation conducted by IDC and an expert panel.[13] We consider that document to be a fair, objective, transparent and thorough assessment of the state of ENISA at the time, and our interviews and cross-checks have found no inconsistencies whatsoever. It represents the only solid bedrock that we have found; however, it describes ENISA as it *was*, not as it *is*.

We conducted far more interviews than were initially planned, and used them to "triangulate", looking for issues and inconsistencies. We sampled the original consultation responses, rather than relying on the Commission's summaries. We relied on the 2007 evaluation report and its appendices, rather than depending on summaries and responses nominally based on the 2006-2007 evaluation.[14,15] We placed only limited reliance on assessments managed by ENISA itself.[16] Wherever possible and practical, we have used original documents, stakeholder interviews and other independent sources rather than relying on summaries that might possibly prove to be slanted.

In the end, we found it necessary to generate what in effect represents an abbreviated current independent evaluation of ENISA as it is today, since none had been conducted since 2007, shortly after the agency began operation.

This suggests a first general recommendation to the European institutions. We introduce each recommendation at the point in the text at which it is relevant, and then collect a list of all recommendations in Section 6 of this report.

Recommendation 1. ENISA should be subject to regular, fully independent evaluations.

ENISA should be subject to a fully independent evaluation not less frequently than twice per Multiannual Financial Framework (MFF) cycle.[17] This would put it on the same calendar as many other European agencies.

We also found it necessary to craft our own abbreviated impact assessment (see Section 5 of this report), rather than relying on the impact assessment[18] that accompanies the Commission's 2010 proposal for modernisation of ENISA.[19]

1.2. Which way forward?

In principle, there is always the question: should the agency continue as it is, should it be abolished, or should it be changed going forward? In this case, the answer at this level of discussion seems to be fairly clear.

[13] Evaluation of the European Network and Information Security Agency: Final Report by the Experts Panel, IDC EMEA, 8 January 2007, http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/index_en.htm.

[14] Communication from the Commission to the European Parliament and the Council: On the evaluation of the European Network and Information Security Agency (ENISA), COM(2007) 285 final, Brussels, 1 June 2007.

[15] Response of the Management Board, at http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1/decision_09.pdf.

[16] See "Measuring uptake of ENISA deliverables in the Member States", available at: http://www.enisa.europa.eu/act/sr/Measuring%20Uptake.

[17] The current MFF cycle ends in 2013. The next runs from 2014-2020.

[18] SEC(2010) 1126, Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1126:FIN:EN:PDF.

[19] 2010/0275 (COD); Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), COM(2010)521 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF.

In the case of ENISA, we think that a widespread consensus has emerged that the agency meets real needs at European level, that it would be challenging and costly to achieve the same ends through interaction among the players at national level, and that an agency such as ENISA is thus the most efficient and appropriate way to achieve the necessary coordination at European level.

It is also fairly clear that continuation of the agency exactly as it is would be inappropriate. First, new challenges and missions for ENISA are emerging all the time, including (1) conducting cybersecurity exercises at European level and optionally in cooperation with the US; (2) coordinating the reporting of breach notifications, as required in the 2009 modifications to the regulatory framework for electronic communications; and (3) interactions with cybercrime, electronic privacy, and other stakeholders in neighbouring policy domains. Second, ENISA faces multiple well-known challenges to its effectiveness and efficiency, many of which ENISA itself cannot correct.

The core questions, then, relate to how ENISA should be changed both to improve its efficiency and effectiveness, and to empower it to deal with new or emerging missions?

1.3. The location of ENISA

Every discussion about ENISA has a strong tendency to begin and end with a discussion of the agency's location in Heraklion, Greece. The European Parliament chose not to include location of the agency in the terms of reference for this study, and we have honoured that decision.

Our terms of reference do, however, require us to consider budget and staffing issues, and to make recommendations as to ways to improve the effectiveness of the agency. The location of the agency clearly plays a role in these required aspects of the study. We have reflected the influence of the agency's location wherever necessary in order to provide an objective and complete assessment.

1.4. Structure of this report

Chapter 2 discusses the evolving European environment in terms of both cybersecurity threats and Critical Information Infrastructure Protection (CIIP). Chapter 3 discusses the structure and history of ENISA, and summarises the various assessments of ENISA's performance that have been conducted. In light of the long time that has elapsed since an independent assessment was last conducted, we have provided our own assessment of the current functioning of the agency. Chapter 4 discusses alternative future courses for ENISA. Chapter 5 is formulated as an abbreviated impact assessment, drawing on the Commission's impact assessment but (as previously noted) with a somewhat different focus. Finally, Chapter 6 provides recommendations.

2. THE GROWING NEED FOR NETWORK AND INFORMATION SECURITY (NIS) IN EUROPE

KEY FINDINGS

- The number of serious Information and Communication Technologies (ICT) related incidents appears to be increasing.
- This has led to additional attention for Network and Information Security from Member States and the EU.
- In recent years, EU initiatives on Network and Information Security (NIS) have broadened in scope to include Critical Information Infrastructure Protection and cyber security.
- All of these developments imply that the relevance of the function that ENISA performs at European level is growing over time.

2.1. Threats

With the increased use of Information and Communication Technologies (ICT) in almost all parts of society, the number and severity of ICT-related threats have increased as well. ICT-related threats may occur in different form, and may include the loss of:[20]

- confidentiality, the property that information is not made available or disclosed to unauthorised individuals, entities, or processes;
- integrity, the property of protecting the accuracy and completeness of assets;
- availability, the property of being accessible and usable upon demand by an authorised entity.

All information held and processed by an organisation is subject to for instance threats of attack, error, technical nature, and nature (for example flood or fire).[21] These threats may affect information systems of e.g. government, businesses, SMEs and citizens.

Because of the increased use of ICT for important business, financial and government information assets, ICT has also grown to attract persons with criminal intentions, activists and state sponsored organisations. This has led to new types of threats like distributed denial-of-service attacks, phishing, spam, identity theft and cyber espionage.

This makes NIS an area of growing concern.

2.1.1. Evolution over time

Although not many reliable facts and figures are known on the number of ICT incidents, many sources show an increase in the both the number and severity of incidents.

One recent study on the cost of cybercrime was performed by Detica in partnership with the Office of Cyber Security and Information Assurance (OCSIA) of the United Kingdom[22].

[20] ISO/IEC 27000:2009 « Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary ».

[21] ISO/IEC 27000:2009 « Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary ».

Their analysis estimated the cost of cybercrime to the UK as £27bn (31 billion euro) per annum in the most likely scenario. A significant proportion of this cost comes from the theft of Intellectual Property (IP) from UK businesses, which is estimated at £9.2bn (10.6 billion euro) per annum. The study also states that in all probability the real impact of cybercrime is likely to be much larger than reported.

Another recent survey on trends in cyber threats was performed by the Dutch CERT organisation, GovCERT.NL.[23] One of the trends described in this report states that cybercrime is becoming more advanced and targeted.[24] Whereas in the infancy years of ICT many of the illegal actions were performed for recreational purposes, in recent years cyberspace has become the playing field of highly organised and technologically advanced criminal organisations.

The difficulty in determining the precise objectives and origin of the attacks and in attributing the attacks to specific organisations can also make cyber-attacks an interesting 'weapon' for activist and state-related organisations.

Recent reports by a number of intelligence services have stated that they see an increase in the number of state sponsored attacks and cyber espionage actions by foreign states and other actors. The national security strategy of the United Kingdom[25] identifies hostile computer attacks on UK cyberspace and large scale cybercrime as one of the highest priority threats for the United Kingdom. The report states that attacks in cyberspace can have a potentially devastating real-world effect. Government, military, industrial and economic targets, including critical services, could feasibly be disrupted by a capable adversary.

Food for thought 1. A growing number of potentially serious cyber-attacks in the UK.

On 7 June 2011, the Defence Secretary of the UK told representatives of UK businesses that the Ministry of Defence blocked and investigated more than 1,000 potentially serious cyber-attacks in 2010. Between 2009 and 2010, security incidents more than doubled.[26]

The German Federal Ministry of the Interior has stated[27] that the number of online espionage and cyber-attacks against German interests were becoming more common and that the number of attacks in the first nine months of 2010 was around 1,600, compared with 900 for all of 2009.

The 2010 annual report of the Dutch General Intelligence and Security Service (AIVD) stated[28] that there is a serious risk of digital attacks on electronic networks and that these attacks are expected to increase in number.

[22] Detica report "The Cost of Cybercrime" (2011), http://www.cabinetoffice.gov.uk/sites/default/files/resources/the-cost-of-cyber-crime-full-report.pdf.

[23] These teams are often called Computer Emergency Response Teams (CERT).

[24] GovCERT.NL, « Nationaal Trendrapport Cybercrime en Digitale Veiligheid 2010 » (Trend report 2010), November 2010, http://www.govcert.nl/binaries/live/govcert/hst%3Acontent/english/service-provision/knowledge-and-publications/trend-reports/trend-report-2010/trend-report-2010/govcert%3AdocumentResource/govcert%3Aresource.

[25] A Strong Britain in an Age of Uncertainty: The National Security Strategy, October 2010.

[26] *Guardian professional*, June 8, 2011.

[27] http://www.dw-world.de/dw/article/0,,14740503,00.html.

[28] https://www.aivd.nl/english/publications-press/@2664/aivd-annual-report.

A recent OECD study[29] analysed whether cyber-incidents could lead to a 'global shock' as devastating as e.g. large-scale pandemics. They concluded that there are a very few cyber-events with the capacity to provoke a global shock. Although they state that there are many examples where cyber-incidents have caused a great deal of harm and financial loss, they conclude that the greatest concern for policy makers are large scale events caused by two different cyber-incidents taking place at the same time or a cyber-event taking place during another form of disaster or attack.

Food for thought 2. Some incidents are on a large scale.

In 2007, Estonia suffered for days from a number of denial-of-service attacks against websites of Estonian organisations, including the Estonian parliament, ministries and banks. The attacks seemed to be organised as a reaction to the relocation of a Russian war memorial statue.

In 2009, details became known about the Ghostnet malware. More than 1000 systems were infiltrated, including ministries of foreign affairs of several countries around the world. Ghostnet malware was able to steal classified information and also reported to be able to access the microphones and webcams of the infected systems.

In 2010, the large botnet Bredolab was dismantled by Dutch police. Bredolab was a large network estimated of around 30 million infected computers that could be controlled from more than 100 command and control servers. This botnet was rented out by the owner to other cyber criminals and was e.g. used to send out malware and spam.

2.1.2. The international dimension

Most ICT infrastructures are strongly internationally connected. In normal traffic across the Internet, routing may include routers and servers in different countries. Because of the architecture of the internet, it is impossible to determine which route data packets have taken or in which country the data is stored. This is especially true for new ICT-developments such as cloud computing.

In light of the international character of cyberspace, criminal cyber-incidents often have an international dimension. Attacks on information systems in one country can be performed by means of ICT infrastructure in a second country which is controlled by criminals in a third country. This makes it hard for European law enforcement agencies to take swift action against cyber criminals, as cross-border support requires proper understanding as to whether the crime that takes place in another country is locally prohibited according the local (cyber) criminal laws.

Food for thought 3. European institutions are not immune 1.

In January 2010, large scale phishing attacks took place against the EU Emissions Trading System (EU ETS) registries. As a result of these phishing emails, a limited number of fraudulent transactions were performed as the fake website appeared genuine.

[29] Reducing Systemic Cybersecurity risk, P. Sommer, I. Brown, IFP/WKP/FGS(2011)3.

2.2. Developments in network and information security

Network and information security consists of processes and measures to protect information and information networks and assets[30]. The protection can take different forms, ranging from pro-active measures like awareness raising, prevention such as the use of firewalls, intrusion detection systems, response team, and well-trained recovery processes. Effective network and information security requires a balance of technological and organisational processes and measures as well as taking care of the human factor.

2.2.1. Evolution over time

In recent years, the focus in network and information security has shifted from prevention to 'defence in depth' and more emphasis on detection and response. Many organisations now have specialised teams for monitoring networks traffic, and responding to incidents.

Recent years have also shown that incidents in the ICT domain can have serious consequences in the physical domain. The Stuxnet incident in 2010 showed that alike malware potentially could lead to serious problems for the functioning of critical infrastructures (CI) such as the energy sector. This emerging threat for CI make Critical Information Infrastructure Protection (CIIP) and cyber security an important topic for policy makers in a number of European Union Member States (MS).

Food for thought 4. Stuxnet was a sophisticated cyber-attack on the physical domain.

In 2010, Stuxnet was discovered. This malware was designed to target specific industrial systems. Its target was widely believed to be Iran's uranium enrichment facility. In light of Stuxnet's complexity, a number of experts have suggested that foreign states must have been involved in its development.

Many countries have recently established national cyber security and cybercrime strategies.

- **United Kingdom**: the UK has developed a cyber security strategy (June 2009) and a cyber-crime strategy (March 2010). The cyber security strategy characterises the criminal use of cyberspace as one of the principal threats to the nation. The cybercrime strategy contains actions to combat cybercrime directly by improving law enforcement response, and indirectly in developing national and international collaboration with industry and other groups.
- **Germany**: the German cybersecurity strategy (February 2011) recognises that the State, critical infrastructures, businesses and citizens in Germany do highly depend on the reliable functioning of ICT.
- **France**: The French Défence et sécurité des systèmes d'information: Stratégie de la France31 was published in February 2011 and deals with cyber security from the perspective of a serious national threat.

[30] Information security is the preservation of confidentiality, integrity and availability of information (ISO/IEC 27000:2009). Network and information security is defined by COM(2001) 298 as "the ability of a network or an information system to resist, at a given level of confidence, accidental events or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted data and the related services offered by or accessible via these networks and systems".

[31] Defence and security of information systems: the French strategy, February 2011.

These national cybersecurity strategies include several action lines, including:

- The review and harmonisation of legislation relevant to cyber security;
- The development of effective procedures and technology to better detect and respond to cybersecurity incidents that threaten the undisturbed functioning of society;
- National collaboration across different parts of government and through close collaboration with private organisations, e.g., in information sharing initiatives;
- Strengthening of the cyber security posture of the critical infrastructures;
- The establishment of specialised cyber security organisations at the strategic and operational levels, including the Office of Cyber Security (OCS) and the Cyber Security Operational Centre (CSOC) in the UK and the recently established Cyber Defence Centre (Nationales Cyber-Abwehr Zentrum) in Germany.[32]

2.2.2. The international dimension

Almost all of these national cyber security strategies stress the fact that for effective cyber security close international collaboration is required on the topics: harmonisation of international regulation, the exchange of information on risk factors, and better and swifter international collaboration in response.

On the other hand, despite the fact that all Member States have signed the Council of Europe Convention on Cybercrime (CETS No.: 185), ratification and entry into force of the harmonised approach to cyber-crime is in a number of cases still pending.[33]

Some platforms for international collaboration exist, e.g. the European SCADA Control Systems Information Exchange (EuroSCSIE) as an international information exchange for Process Control Systems (PCS) security and the international Computer Incident Response team community.

2.3. Network and information security within the EU

2.3.1. The Network and Information Security strategy

Network and Information Security (NIS) has been on the agenda for EU policy makers already since the 2001 Communication of the European Commission on NIS[34].

In 2006, the European Commission aimed to give new momentum to European NIS by developing a strategy for a secure information society. The approach was based on a dialogue to bring together all stakeholders.[35] The pillars of this approach were dialogue, partnership and empowerment.

2.3.2. The tasks of ENISA in regard to Network and Information Security

In 2004 the European Network Information Security Agency (ENISA) was established by Regulation EC 460/2004 to enhance NIS in Europe. ENISA was tasked to contribute to the

[32] It opened on 16 June 2011. See: https://www.bsi.bund.de/ContentBSI/Presse/Pressemitteilungen/Presse2011/Eroeffnung-Nationales-Cyber-Abwehrzentrum_16062011.html.

[33] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.

[34] COM(2001)298, Network and Information Security : proposal for a European Policy approach.

[35] COM(2006)251, A strategy for a secure Information society – dialogue, partnership and empowerment.

development of a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations throughout the European Union.[36]

In the 2006 strategy on the secure information society,[37] the role of ENISA was described as essential. ENISA's role was seen as a possible centre for information sharing, co-operation amongst all stakeholders, and the exchange of commendable practices, both within Europe and with the rest of the world (see Section 3.1).

2.3.3. Critical Information Infrastructure Protection (CIIP), cyber security and the Digital Agenda for Europe (DAE)

After the large-scale cyber-attacks on Estonia, an EU initiative on Critical Information Infrastructure Protection (CIIP) was established in 2009.[38] This initiative was specifically aimed to strengthen the security and resilience of critical ICT-infrastructures by stimulating and supporting the development of a high level of preparedness, security and resilience capabilities both at the national and European levels.

The Action Plan launched by the CIIP Communication introduced two platform organisations:

- European Forum for information sharing between Member States (EFMS) to share information and good policy practices on security and resilience of Critical Information Infrastructures (CII);
- The European Public Private Partnership for Resilience (EP3R), a co-operation platform between the public and private sector on security and resilience objectives, baseline requirements, good policy practices and measures.

Trust in cyberspace and cyber security are also seen as essential for achieving the Digital Agenda for Europe (DAE). Pillar III of the Digital Agenda action plan concerns "Trust and Security". The DAE includes the reinforcement of Network and Information Security, the establishment of a cybercrime platform, and support to EU-wide cyber security preparedness. The DAE aims to set up a European rapid response system to cyber-attacks, including a well-functioning network of Computer Emergency Response Teams (CERTs).

The DAE aims to propose tougher laws to combat cyber-attacks against information systems and work on related rules on jurisdiction in cyberspace at European and international levels.

The 2011 CIIP Communication[39] takes stock of the results achieved since the adoption of the CIIP action plan of 2009. It underlines the important role of EFMS and EP3R and describes the next steps for EFMS, EP3R as well as ENISA's role. It states that in the long term and in line with the proposal for a new ENISA Regulation, it is envisaged that EP3R should become a key activity of a modernised ENISA.

2.3.4. Relationship with data protection

Cyber security and electronic privacy tend to be interlinked in complex ways. Most cyber security measures depend on *authentication* (which ensures that a user is who he or she

[36] Regulation 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

[37] COM(2006)251, A strategy for a secure Information society – dialogue, partnership and empowerment.

[38] Communication on Critical Information Infrastructure Protection – Protecting Europe form large scale cyber-attacks and cyber-disruptions : enhancing preparedness, security and resilience, COM (2009) 149.

[39] Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security', COM (2011) 163.

purports to be) and *authorisation* (which determines whether the identified user has the right to do that which he or she wishes to do). Authentication and authorisation thus inherently relate to the individual.

Personal data is widely stored online these days, and large scale data breaches can occur. The proliferation of social networks and other online activities potentially exposes not only information that is intended to be generally available, but also information that is intended to be available only to a limited circle of individuals. Technological developments and globalisation are key drivers for the on-going revision of data protection rules.[40]

Food for thought 5. Personal data could be exposed to cyber-attacks.

"Sony is investigating another hacking attack on one of its websites. A group called Lulz Security claims to have broken into Sonypictures.com and accessed details of a million users. Passwords, home addresses and other personal information relating to several thousand of the accounts was released online. It is the third major hack to hit Sony since April when the PlayStation Network was targeted and the details of 77 million users compromised."[41]

ENISA is inevitably being drawn into a number of activities that have privacy implications, and this is likely to increase. Security measures are also a key element in data protection.

ENISA's work programme for 2011 contains several items related to privacy, including an analysis of the security and privacy issues of new technologies such as the Internet of Things, cloud computing, and smart phones (WKP2.1), promoting a Pan-European approach to privacy and trust-establishment models (WPK3.2), and continuing support to the review and implementation of the e-Privacy Directive[42] (WPK3.3).

In WPK 3.3, ENISA reviewed[43] the situation with respect to the EU data breach notification requirement for the electronic communications sector in the e-Privacy Directive (2002/58/EC), and worked on guidelines on how to implement measures and procedures as described by Article 4 of the e-Privacy Directive.

Some of ENISA's tasks related to incident reporting and data collection may require enforcement of data protection rules by the agency itself.

The 2009 revision of the Telecommunications Regulatory framework[44] introduced provisions aimed at strengthening obligations for operators to ensure security and integrity of their networks and services. Among other measures, the revised framework introduced an obligation for undertakings providing e-communication services to report security incidents with a significant impact on the operation of networks or services to Member State authorities. It calls on ENISA to assist the Commission as appropriate in developing technical implementing measures to ensure, for instance, consistency of reporting. ENISA is

[40] Commission Communication on 'A comprehensive approach on personal data protection in the European Union', COM(2010) 609 final.

[41] BBC news, June 3, 2011, http://www.bbc.co.uk/news/business-13636704.

[42] Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector (e-Privacy Directive) as amended by Directive 2009/136/EC (Citizens' Rights Directive).

[43] www.enisa.europa.eu/act/it/dbn.

[44] See Article 13a of the Framework Directive, 2002/21/EC as amended by Directive 2009/140/EC (Better Regulation Directive).

already working in collaboration with regulatory authorities on procedures for incident reporting, and on a unified scheme for reporting to ENISA and European Commission.[45]

It is not yet altogether clear whether ENISA's role with respect to incident reporting includes the transmission, handling and storing of sensitive information and personal data. The European Data Protection Supervisor has therefore asked for a clarification on whether ENISA will be processing personal data.[46] If sensitive and personal data is involved, trust building and appropriate protection of this data will be one of the key elements of this activity.

2.3.5. Relationship to cybercrime

In addition to the initiatives on the security for the Information Society, parallel European initiatives were made to fight cybercrime. The main elements of the Communication on cybercrime[47] were increased law enforcement co-operation, public-private partnership and international co-operation.

Combatting cybercrime is also a high priority topic of the Digital Agenda for Europe (DAE). In the action area focused on trust and security, the Commission is committed to measures to combat cyber-attacks against information systems. The DAE includes the establishment of a European cybercrime platform (action 30), a study on the feasibility and usefulness of a pan-European cyber crime centre (action 31), promoting the fight against cybercrime at the international level (action 32) and setting-up national alert platforms with links to the EUROPOL cybercrime platform (action 41).

The Commission's 2010 proposal[48] on attacks against information systems is aimed, inter alia, to deal with large-scale cyber-attacks against businesses and governments. Its main element is the penalisation of the use as well as the production and sale of tools to commit attacks against information systems.

Important stakeholders in the fight against cybercrime are the national and international law enforcement agencies. In this field, collaboration exists e.g. through international organisations as EUROPOL and EUROJUST.

At its 26 April 2011 meeting, the Council of the EU reached conclusions concerning an action plan to implement the concerted strategy to combat cybercrime.[49] One of the conclusions was to promote relationships with European agencies including EUROPOL, EUROJUST and ENISA in order to reach a better understanding of the trends and modus operandi of cybercrime.

2.4. The role of Computer Emergency Response Teams (CERTs)

2.4.1. The tasks of CERTs

The growing number of cyber incidents require a more active and organised form of response. For this response, Computer Emergency Response Teams (CERTs)[50] play an

[45] www.enisa.europa.eu/act/res/files/reporting-major-security-incidents-implementation-of-article-13a/view.

[46] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (2011/C 101/04).

[47] Commission communication COM(2007) 267 final "Towards a general policy on the fight against cyber-crime" (2007).

[48] COM(2010) 517 final, Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA.

[49] www.consilium.europa.eu/uedocs/cms_data/.../114028.pdf.

[50] A more general term is Computer Security Incident Response Teams (CSIRT). The term CERT is protected and registered as a trademark by the CERT Coordination Center and Carnegie Mellon University. However, for the purpose of this study we use the term CERT which may be more familiar to our readers.

important role. A CERT is an organisation which provides services and support for their constituency for the prevention, handling, and response to cyber security incidents.

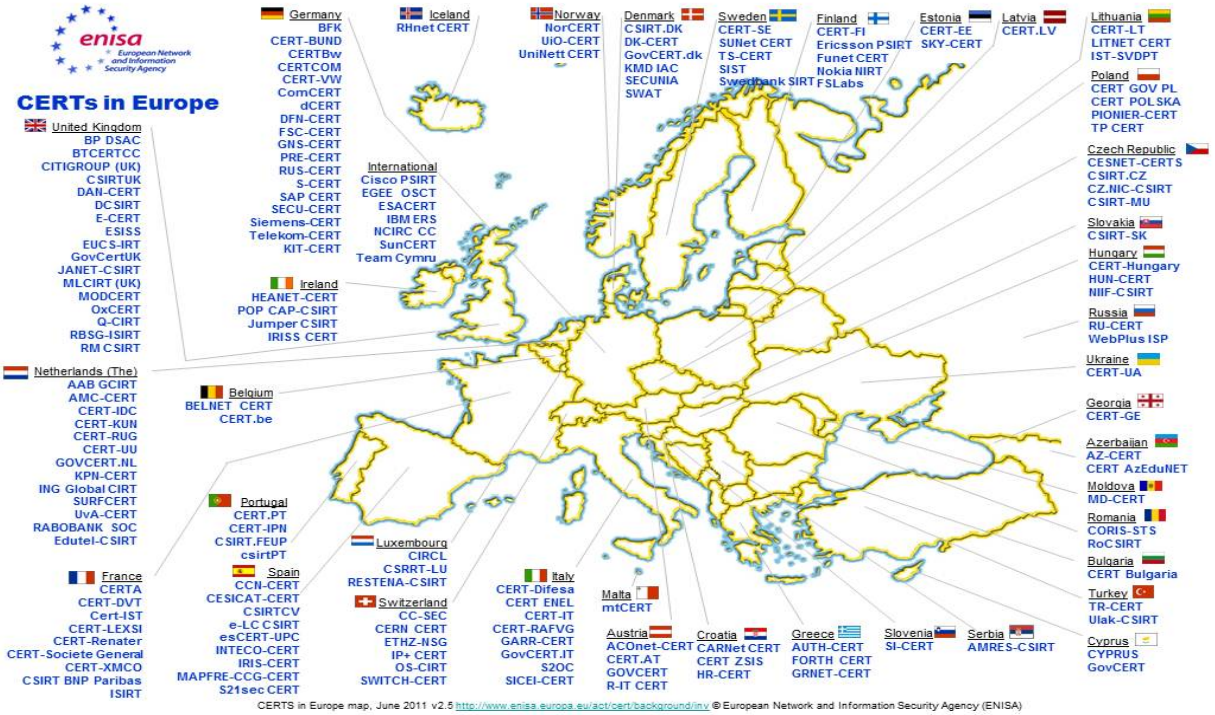
Around the world, there exist several hundred CERT organisations which serve a variety of constituents, including commercial, academic, government and military organisations. Europe is served by a substantial number of CERTs (see Figure 1).

Tasks of these types of CERTs may include:

- gathering information and disseminate knowledge on information security threats and incidents;
- giving recommendations, advice and guidelines for improvement of information security;
- helping to solve information security problems;
- co-ordination of the response in case of ICT-related incidents; and
- maintaining contact and sharing information with other CERTs.

Some CERTs have the national government as their constituency. These national CERTs have a broad national responsibility. Some countries recognised the need to not only protect governmental networks but also to protect national critical infrastructure. These national CERTs are established to co-ordinate the response to large scale cyber incidents, to gather information on cyber incidents, and to act as an international point of contact for other CERTs.

Figure 1: CERTs in Europe[51]



Source: ENISA web site

[51] Source: ENISA web site at http://www.enisa.europa.eu/act/cert/background/inv/files/certs-in-eurioe-map.

2.4.2. Possible Computer Emergency Response Team (CERT) for the European institutions

For all major networks that may face large scale attacks, the services of a CERT can have added value.

Food for thought 6. European institutions are not immune 2.

In March 2011, a group of hackers attacked the European Commission (EC) and the European External Action Service. The attack took place just before the EU leaders' summit in Brussels. An EC spokesman explained that it was a "targeted attack" against the correspondence of "certain Commission officials". It also became known that all the Commission officials had been asked to change their email passwords, and that they were for the time being unable to access their official email accounts outside the Commission buildings. The European Parliament also reported problems.[52]

It is therefore useful that a CERT cover the main networks of the European institutions. In June 2011, a CERT pre-configuration team was launched "… to counter the threat of cyber-attacks against the EU institutions, bodies and agencies. The team is made up of IT security experts from the EU institutions. At the end of one year's preparatory work by the team, an assessment will be made leading to a decision on the conditions for establishing a full–scale CERT for the EU institutions."[53]

The CERT pre-configuration team will operate in close cooperation with the IT security teams in the respective EU Institutions and liaise with the community of CERTs in the Member States and elsewhere, exchanging information on threats and how to handle them.

For this collaboration, the European Government CERTs (EGC)[54] group could play an important role. The EGC group is an informal group that is developing effective co-operation on cyber incident response matters between its members. The EGC is an operational group with a technical focus. Currently, the EGC consists of CERTs in twelve countries. The EGC teams actively participate in ENISA activities, particularly in relation to the formation of government CERTs in Europe.

2.4.3. Current ENISA role with respect to Computer Emergency Response Teams (CERTs)

ENISA's is not a CERT organisation and the agency's role is not operational. ENISA acts as a facilitator and information broker for CERTs or Computer Security Incident Response Teams (CSIRTs).

Some of the activities of ENISA in this area are:[55]

- "Initiating contact with relevant global players in the CERT field. The Agency has met representatives from FIRST, TF-CSIRT, the American CERT/CC, Asian-Pacific-CERT and the National Computer Network Emergency Response Technical Team/Coordination Centre of China;

[52] http://www.euractiv.com/en/future-eu/cyber-attack-european-commission-reported-news-503461.
[53] http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694.
[54] http://www.egc-group.org.
[55] http://www.enisa.europa.eu/act/cert.

- Collecting and disseminating good practices, e.g., in its publications Step-by-Step Approach on How to Establish a CSIRT and Good Practices for Running a CSIRT;
- Providing an overview on the actual situation concerning CERT matters in Europe. It provides a list of response teams and similar facilities by country, but also contains a catalogue of co-operation, support and standardisation activities related to them;
- Developing a set of policy recommendations on baseline capabilities of national/governmental CSIRTs;
- Describing good practices as well as providing practical information and guidelines for the management of network and information security incidents with an emphasis on incident handling."

2.5. Critical infrastructure protection (CIP)

Critical infrastructures (CI) such as the electrical grid and the rail transport are increasingly dependent on ICT. Critical Infrastructure Protection (CIP) and cyber security are related in two ways:

- Many ICT infrastructures are essential for the functioning of society, and therefore nationally designated as CI. Various parts of the ICT sector are part of the National Critical Infrastructure of several of the Member States. Currently, there is a study on-going on which part of the ICT infrastructure should be designated as part of the European Critical Infrastructure (ECI).[56]
- ICT vulnerabilities and cyber-attacks are one of the possible risk factors for all CI. Many countries include protection against these vulnerabilities as an important action of their CIP programmes.

The emerging threat of cyber-attacks against CI makes Critical Information Infrastructure Protection (CIIP) an important topic in a number of EU Member States. As ICT-based services are increasingly provided at different levels of a value chain by a large number of organisations which include CI operators, cyber security is no longer something which can be completely solved by one organisation alone. The connected web of information services and local processing (e.g., chip cards, transport tokens, in-car systems) require a networked approach by a manifold of organisations such as manufacturers, regulators, policy-makers, operators, law enforcement when dealing with cyber security. As part of the CIP activities, several European countries have established platforms for trusted information sharing on cyber related threats and risk, e.g. CPNI in the UK and CPNI.nl in the Netherlands. Public-private collaboration is an essential part of all CIP efforts.

2.6. International co-operation

International cooperation in regard to NIS has many dimensions, and potentially involves a great many international institutions.

[56] 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.

2.6.1. G8, OECD, OSCE

Cyber security and CIIP are important topics for a number of international organisations, including:

- G8: The G8 are involved with CIIP and cyber security. In 2003, for example, the G8 Justice and Interior Ministers adopted the G8 Principles for Protecting Critical Information Infrastructures.[57] These principles advise countries inter alia to raise awareness, promote partnerships between public and private stakeholders, facilitate tracing attacks, and conduct training and exercises. Other initiatives include the subgroup on High Tech Crime, and the High-tech Crime 24-Hour Point-of-Contact Network.
- OECD: In 2008 the OECD adopted the recommendation of the council on the protection of critical information infrastructures.[58] This document was developed by the OECD Committee for Information, Computer and Communication Policy (ICCP Committee), and its Working Party on Information Security and Privacy. The main points of this recommendation include the protection of critical information infrastructures at the domestic level by demonstrating government leadership and commitment to protect CII, managing the risks to CII, and working in partnership with the private sector; and the protection of critical information infrastructures across borders by cross-border cooperation among countries and with the private sector at the strategy, policy and operational levels.
- The Organization for Security and Cooperation in Europe (OSCE) organised a conference in May 2011 on "A comprehensive approach to cyber security: Exploring the future OSCE role".[59] The conference discussed the potential future role of the OSCE in the domain of cyber security building on their expertise of confidence building measures, and being a unique platform for sharing expertise, good practices and raising awareness of cyber threats and potential responses.[60]

2.6.2. NATO

The cyber threat stood out as an area which NATO needs to address in the study by NATO-appointed Group of Experts on the Alliance's strategic concept. The 2010 NATO Summit in Lisbon also placed cyber security at the forefront of the new security challenges that NATO confronts. In March 2011 the framework for a Concept on NATO's Cyber Defence was agreed by NATO defence ministers.

Main NATO cyber defence elements are the following:

- the NATO Cyber Defence Management Authority (CDMA) was established to coordinate cyber defence throughout NATO Headquarters and its associated commands and agencies;
- the NATO Computer Incident Response Capability (NCIRC) provides CERT services for the NATO networks;
- NATO's Cooperative Cyber Defence Centre of Excellence (CCD CoE), an international centre of expertise located in Estonia.

[57] http://www.usdoj.gov/criminal/cybercrime/g82004/G8_CIIP_Principles.pdf.
[58] http://www.oecd.org/dataoecd/1/13/40825404.pdf.
[59] http://www.osce.org/event/cyber_sec2011.
[60] http://www.osce.org/cio/77481.

2.6.3. The EU-US working group on cyber security and cybercrime

The USA gives cyber security priority and actively seeks collaboration with international partners. In the recently released strategy[61] the US states that it wishes to co-operate with other countries and that cyber security is an "obligation" for governments and societies. The US already collaborates bilaterally with a number of countries.

In order to strengthen cooperation between the EU and US, an EU-US working group was established at the EU-US summit in November 2010. The working group deals with developing collaborative approaches for the following topics: incident response capabilities, sharing of good practices with the private sector, awareness raising, removing child pornography, and advancing the Convention on Cybercrime.[62] The Working Group will report to the next EU-US Summit, which will take place at the end 2011. The collaboration on incident response capabilities will lead to a joint EU-US cyber-incident exercise by the end of 2011.

2.6.4. Council of Europe

One of the main international instruments on cybercrime is the Convention on Cybercrime of the Council of Europe. The Council of Europe Convention on Cyber Crime (2001) has been ratified by 31 nations and signed by another 16 European and other nations.[63] The Convention arranges for international harmonisation of cyber-crime penal law, multi-national collaboration to stop cyber-crime in progress and to pursue international cyber criminals. The law has to be implemented in the national legal system. The Convention allows certain articles to be implemented in a weaker and stronger way; in addition a nation has to communicate to the other nations which implementation has been chosen. The Convention is still being implemented by some countries.[64]

An additional protocol making any publication of racist and xenophobic propaganda via computer networks a criminal offence has been ratified by fewer nations.[65]

2.6.5. Coordinating cyber security

The short overview of activities in this section shows that cyber security is a broad theme where many initiatives are evolving, and which requires strong international collaboration and adequate EU participation in a large number of initiatives. The broad topic of cyber security is still being defined and many organisations are analysing the importance of Critical Information Infrastructures and developing adequate protection and response measures.

Coordinated EU participation is required in for instance:

- The establishment of principles as e.g. by the G8 and OECD;
- The development and promotion of international agreements, e.g. for the cybercrime convention;
- Collaboration with third countries in exchange of good practices;

[61] International strategy for cyberspace, Prosperity, Security, and Openness in a Networked World, May 2011.
[62] http://europa.eu/rapid/pressReleasesAction.do?reference=MEMO/11/246.
[63] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CL=ENG.
[64] http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm.
[65] http://conventions.coe.int/Treaty/EN/Treaties/html/189.htm.

- Collaboration with industry and supporting industry in taking their responsibility in more reliable networks and products.

A strong EU collaboration in these areas requires a coordinated approach across EU institutions, across Member States, and in collaboration with industry.

One of the main challenges for coordinating cyber security lies in the response to large-scale cyber-attacks against information systems. In November 2010 ENISA facilitated a pan European exercise in which 22 countries actively participated, with participants from inter alia CERTs, Ministries, and cyber-crime units. The exercise showed that the participants had difficulties in contacting the other agencies. The agencies also did not handle incidents reports in the same way, which made it problematic to exchange the information rapidly.

3. ENISA TODAY

KEY FINDINGS

- ENISA's function is increasingly seen as valuable and necessary.
- Under a generally flexible charter, ENISA's effective mission has steadily grown.
- ENISA faces two inherent challenges in regard to efficiency: (1) a small staff size, which inherently implies a relatively high ratio of administrative staff to total staff (see Section 3.3.3.5); and (2) a relatively inaccessible location that implies high travel costs (see Section 3.3.3.8) as well as challenges to recruiting and retention.
- As regards the ratio of administrative staff to total staff, ENISA is now on a par with its peer group of decentralised agencies with fewer than 75 employees.
- The crucial issue with respect to travel is not the travel expenses themselves, but rather the lost time for key knowledge workers, which implies a substantially reduced number of missions per year.
- When one considers that ENISA suffers both from small size and a remote location, the agency faces among the greatest combined challenges to efficiency of any European decentralised agency.

This chapter summarises ENISA's mission, discusses the organisation of ENISA and its related organisations (including the Management Board (MB) and the Permanent Stakeholders' Group (PSG)), and concludes with an in-depth review of the various evaluations of ENISA that have been conducted.

3.1. ENISA's evolving mission

Drawing on the language of the Regulation that established the agency,[66] ENISA describes its functions succinctly:

"The prime purpose of ENISA is to enhance the capability of the Community, the Member States and, as consequence, the business community to prevent, address and respond to network and information security problems.

To this end, ENISA is focusing its activities on:

- "Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks;
- Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field." [67]

[66] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Article 27.

ENISA's role can be understood at two mutually complementary but distinct levels: (1) at the level of what its formal charter authorises it to do; or (2) at the level of what it is actually doing. ENISA's initial objectives and tasks are defined in the 2004 Regulation that established ENISA.[68] The ENISA Regulation provides a broad framework of tasks, leaving considerable discretion to ENISA staff and the ENISA Management Board (subject to approval by the Commission) to determine the specific activities that ENISA will undertake in the coming year. ENISA's actual activities have expanded considerably since it was founded in 2004. Thus, an understanding of the Regulation is a necessary starting point for understanding ENISA's mission, but it is by no means the end of the story.

As previously noted, the Commission put forward a new proposed regulation in 2010 in an effort to streamline and modernise ENISA. Rather than a series of amendments, the new proposed Regulation is a substantial re-write of the old, thus making comparison complex. We consider it useful to compare the old formulations of ENISA's missions to the proposed new ones. Note, however, that the Commission's proposal is at this point a proposal, and that we do not take it as a given for purposes of this study.

Category of tasks	ENISA Regulation (2004)	Commission Proposal (2010)
Collect information and analyse	a) collect appropriate information to analyse current and emerging risks and, in particular at the European level, those which could produce an impact on the resilience and the availability of electronic communications networks and on the authenticity, integrity and confidentiality of the information accessed and transmitted through them, and provide the results of the analysis to the Member States and the Commission;	(c) Assist the Member States and the European institutions and bodies in their efforts to collect, analyse and disseminate network and information security data; (d) Regularly assess, in cooperation with the Member States and the European institutions, the state of network and information security in Europe;
Awareness raising	(e) contribute to awareness raising and (…);	
Collect, develop and promote good practices and standards	d) facilitate cooperation between the Commission and the Member States in the development of common methodologies to prevent, address and respond to network and information security issues; (e) (…) and the availability of timely, objective and comprehensive information on network and information security issues for all users by, *inter alia*, promoting exchanges of current best practices, including on methods of alerting users, and seeking synergy between public	(f) Assist the Union and the Member States in promoting the use of risk management and security good practice and standards for electronic products, systems and services;

[67] ENISA web site, at: http://www.enisa.europa.eu/media/faq-on-enisa/general-faqs-on-enisa.

[68] Regulation (EC) 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency.

Category of tasks	ENISA Regulation (2004)	Commission Proposal (2010)
	and private sector initiatives; (g) track the development of standards for products and services on network and information security; i) promote risk assessment activities, interoperable risk management solutions and studies on prevention management solutions within public and private sector organisations;	
Support collaboration	(c) enhance cooperation between different actors operating in the field of network and information security, *inter alia*, by organising, on a regular basis, consultation with industry, universities, as well as other sectors concerned and by establishing networks of contacts for Community bodies, public sector bodies appointed by the Member States, private sector and consumer bodies;	(e) Support cooperation among competent public bodies in Europe, in particular supporting their efforts to develop and exchange good practices and standards; (g) Support cooperation between public and private stakeholders on the Union level, inter alia, by promoting information sharing and awareness raising, and facilitating their efforts to develop and take up standards for risk management and for the security of electronic products, networks and services; (h) Facilitate dialogue and exchange of good practice among public and private stakeholders on network and information security, including aspects of the fight against cybercrime; assist the Commission on policy developments that take into account network and information security aspects of the fight against cybercrime;
• Collaboration with industry	(f) assist the Commission and the Member States in their dialogue with industry to address security-related problems in the hardware and software products;	
• Collaboration between MS		(b) Facilitate the cooperation among the Member States and between the Member States and the Commission in their efforts with a cross-border dimension to prevent, detect and respond to network and information security incidents;
Advice on NIS to the Commission and other EU institutions	b) provide the European Parliament, the Commission, European bodies or competent national bodies appointed by the	(a) Assist the Commission, at its request or on its own initiative, on network and information security policy development by providing it

Category of tasks	ENISA Regulation (2004)	Commission Proposal (2010)
	Member States with advice, and when called upon, with assistance within its objectives; h) advise the Commission on research in the area of network and information security as well as on the effective use of risk prevention technologies	with advice and opinions and with technical and socio-economic analyses, and with preparatory work for developing and updating Union legislation in the field of network and information security; (i) Assist the Member States and the European institutions and bodies, at their request, in their efforts to develop network and information security detection, analysis and response capability;
Collaboration with third countries	(j) contribute to Community efforts to cooperate with third countries and, where appropriate, with international organizations to promote a common global approach to network and information security issues, thereby contributing to the development of a culture of network and information security;	(j) Support Union dialogue and cooperation with third countries and international organisations in cooperation where appropriate with the EEAS, to promote international cooperation and a global common approach to network and information security issues;
Other tasks	(k) express independently its own conclusions, orientations and give advice on matters within its scope and objectives.	(k) Carry out tasks conferred on the Agency by Union legislative acts.

Source: Study team

Comparing the tasks in the 2004 Regulation with those in the Commission's proposed new Regulation, we make the following observations:

- Both task lists represent the main line of ENISA's activities in the area of NIS good practices; however, the tasks of the Commission proposal seem in general to be formulated more broadly, and yet in a way that implies less direct responsibility. This holds especially for the development and promotion of good practices and standards (but also elsewhere), where the task descriptions seem to shift from an active implementation role to a more supporting and facilitating role.
- The tasks in the Commission proposal show more focus on the support of the Commission and Member States, and less focus on industry or users, as shown for example by less emphasis on awareness raising activities, and less explicit mention of industry, consumer bodies, and users as a target group.
- Task b and Task i in the Commission proposal reflect the growing need and attention for the prevention, detection and response to cross-border incidents.
- Task h of the Commission proposal reflects a broadened scope, by including the NIS aspects of the fight against cybercrime.
- The tasks of the Commission proposal do not contain explicit reference to data protection.

- The tasks of the Commission proposal do not explicitly mention incident reporting and data collection by ENISA (despite the fact that the Framework Directive, as revised in 2009, assigns breach notification data collection tasks to ENISA). This may lead to lack of clarity with respect to possible consequences of these tasks on data protection and security requirements.69
- Task h from the 2004 Regulation on providing advice on the research agenda is not reflected in the Commission proposal.

With that established, it is useful to view the activities of the agency, bearing in mind that they are required to fall within the broad ambit established by the 2004 Regulation. Activities include:

- Activities that ENISA has performed for many years, such as collecting and promoting good practices, providing advice to the Commission and Member States on NIS related topics; and support for the CERTs (see Section 2.4),
- Through the 2009 CIIP Communication,[70] liaison with both the European Public Private Partnership for Resilience (EP3R) and the European Forum for information sharing between Member States (EFMS) in regard to CIIP (see Section 2.3.3).
- As another reflection of the 2009 CIIP Communication, conducting exercises at European level in 2010 and with the US in 2011 (see Section 2.6.5).
- Assisting with breach notification data as envisioned in the Framework Directive as revised in 2009 (see Section 2.3.4).
- Participating in the expert group that is evaluating the creation of a CERT for the European institutions beginning in 2011 (see Sections 2.4.2).
- Interaction with data protection stakeholders, primarily since 2010, and with cybercrime stakeholders and groups in order to exchange best practice (see Sections 2.3.4 and 2.3.5). This is to some extent already the case, but we assume that existing restrictions in the 2004 Regulation would be eased or eliminated.
- Interaction with a range of international stakeholders and bodies (see Section 2.6).

3.2. ENISA's organisation

The 2004 Regulation establishes the European Network and Information Security Agency (ENISA) and describes the main elements of its structure: the agency itself (see Section 3.2.1), headed by an Executive Director, the Management Board (see Section 3.2.2), and a Permanent Stakeholders Group (PSG) (see Section 3.2.3). Section 3.2.4 discusses other aspects of ENISA's organisation, while Section 3.2.5 summarises ENISA's current budget.

[69] Opinion of the European Data Protection Supervisor on the proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA) (2011/C 101/04). See also Section 4.2.3.

[70] Commission Communication on Critical Information Infrastructure Protection "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience", COM(2009) 149 final, 30 March 2009. See also the Commission Communication on Critical Information Infrastructure Protection 'Achievements and next steps: towards global cyber security' COM (2011) 163.

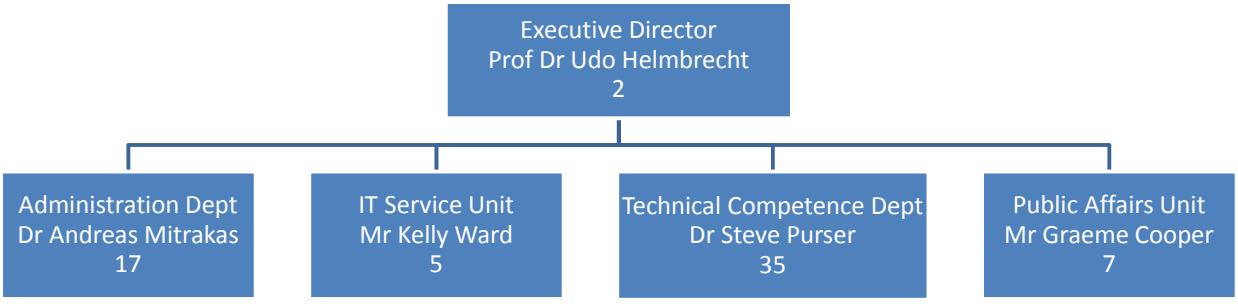
3.2.1. The agency

The Executive Director (ED) is responsible for managing the Agency. The current Executive Director, Dr. Udo Helmbrecht, has been in charge since October 2009. He was nominated by ENISA's Management Board and appointed in April 2009.

The agency as currently structured consists of four departments, as depicted in Figure 2. Each box contains the name of the unit, the name of the manager, and the number of allocated staff.[71] Note that the larger entities (Administration, and Technical Competence) are referred to as *Departments*, while smaller entities at the same reporting level (Public Affairs, IT Services) are referred to as *Units*.

- The Administration Department ensures compliance and service in its areas of competence, which comprise of finance, human resources, IT infrastructure and legal services including procurement.
- IT Services is an autonomous unit that is responsible for delivering IT services to the Agency in support of its day to day operations.
- The Technical Competence Department manages technical, security competence issues. Where the technical, methodological and organisational aspects of Network and Information Security are concerned, the Department analyses problem areas, provides advice, demonstrates its proposed solutions and disseminates its work to maximize the impact of the solutions proposed. In the area of external relations, the Department is responsible for awareness raising and liaison with the computer incident response community.
- The Public Affairs Unit is responsible for promoting ENISA's profile by increasing visibility with key actors at political and strategic level, administering communication and outreach channels (ENISA corporate website and digital communication, ENISA publication and information materials), administering media relations, co-ordinating conferences and events, as well as internal communication, as appropriate and as authorised by the Executive Director.

Figure 2: ENISA agency staff and organisation



Source: Study team, based on information provided by ENISA

[71] The number of employees shown here include not only budgeted headcount, but also seconded national experts (SNEs) and trainees. They sum to 66, which is greater than the budgeted headcount of 57.

3.2.2. The Management Board (MB)

The Management Board (MB) consists of a chair and vice chair and representatives from the Commission (3), Member States (27), Stakeholders (3), and EEA countries (3 observers). There are thus 36 MB members in all.[72]

The tasks of the Management Board include:[73]

- the establishment of the budget,
- verification of its execution,
- adoption of the appropriate financial rules,
- establishment of transparent working procedures for decision-making by the Agency,
- approval of the Agency's work programme,
- adoption of its own rules of procedure and the Agency's internal rules of operation,
- appointment and removal of Executive Director.

In 2011, the Management Board meets formally twice a year. In addition one informal meeting and one joint MB-PSG meeting will be organised[74].

The Commission proposal for the modernisation of ENISA seeks to strengthen the supervisory role of the Agency's Management Board and to simplify its procedures (see Section 4.1).

3.2.3. The Permanent Stakeholders Group (PSG)

The Permanent Stakeholder's Group is composed of experts representing the relevant stakeholders, such as Information and Communication Technologies industry, consumer groups and academic experts in network and information security. The PSG is composed of 30 high-level experts from all over Europe who are appointed by the Executive Director for a period of maximum 2.5 years.

The PSG is an expert sounding board for ENISA. The PSG may give advice to the Executive Director in, for example, strategic decisions, drawing up a proposal for the Agency's work programme as well as in ensuring communication with the relevant stakeholders on all issues related to the work programme.

In 2011, as in the past, two formal meetings will be organised; in 2011, joint informal meetings of sub-groups will be held with the Management Board as and when required.

3.2.4. Other mechanisms

Member States representatives - one from each EU and EEA country - are part of the *National Liaison Officers (NLO)* network. A representative from the European Commission and a representative from the Council of the European Union are also part of the NLO network. The NLOs serve as an important point of reference between ENISA and the Member States on specific issues. For some countries, the member of the MB is also part of the NLO network.[75]

In 2011, the NLO network will be expanded to include more differentiated networks of general policy and specific regulatory contacts developed.

---

[72] The chair and vice chair are also members.

[73] http://www.enisa.europa.eu/about-enisa/structure-organization/management-board.

[74] ENISA, work programme 2011, Securing Europe's Information Society, final version – 30 November 2010.

[75] The NLO network is being transformed into a network of National Contact Officers (NCO).

3.2.5. Budget

In order to carry out its tasks, the Agency has a budget of 8.103 million Euros for the year 2011. The expenditure of the Agency includes staff (Title 1), administrative and infrastructure (Title 2), as well as the operational expenditure (Title 3), linked to the Agency's activities.

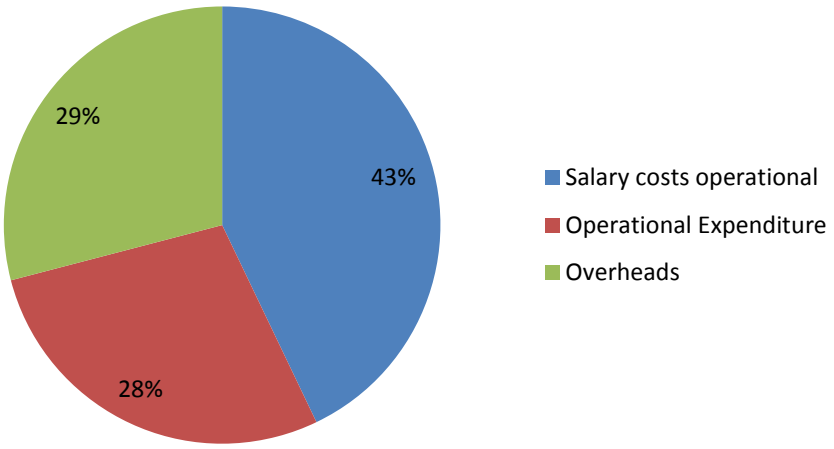
ENISA staff have provided an Activity Based Budgeting view of the 2011 budget (see Table 1). These figures are based on the approved 2011 budget, and thus represent actual rather than proposed allocations.

Table 1: Activity Based Budgeting (ABB) view of ENISA's 2011 budget.

	Staff FTE	Salary costs operational	Operational Expenditure	Overheads	Total Cost
WS1 Facilitator of cooperation	9	€ 733,974	€ 596,000	€ 515,565	€ 1,845,548
WS2 Competence Centre for securing current and future technology	8.5	€ 688,886	€ 390,000	€ 469,438	€ 1,548,333
WS3 Promoter of privacy and trust	6	€ 467,073	€ 304,000	€ 321,717	€ 1,092,796
Total work streams	23.5	€ 1,889,933	€ 1,290,000	€ 1,306,720	€ 4,486,677
Stakeholder relations	3	€ 252,118	€ 300,000	€ 164,654	€ 716,775
Public affairs	4.5	€ 372,455	€ 190,000	€ 243,244	€ 805,704
Missions and representation	0	€ -	€ 438,000	€ -	€ 438,000
Project support activities	3	€ 206,652	€ 10,000	€ 148,305	€ 364,960
Management and Support Activities	9	€ 753,672	€ 44,957	€ 492,210	€ 1,290,848
Total non-workstream	19.5	€ 1,584,897	€ 982,957	€ 1,048,413	€ 3,616,287
Grand total	43	€ 3,474,830	€ 2,272,957	€ 2,355,133	€ 8,102,963

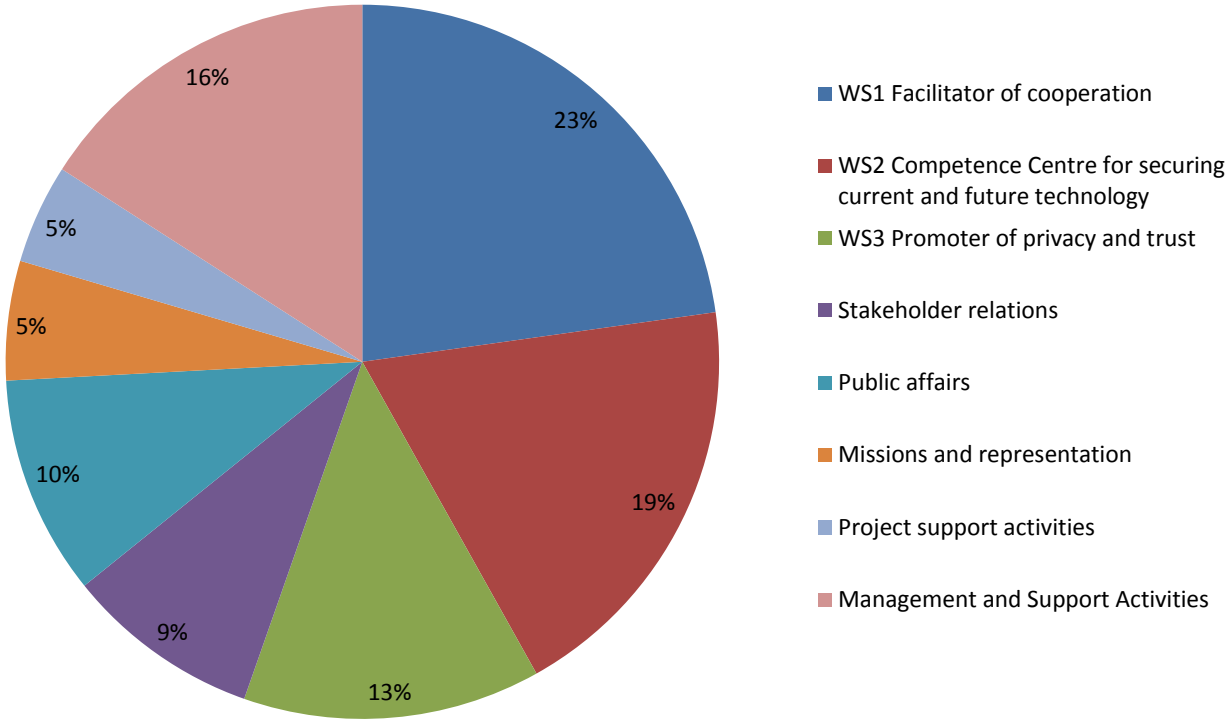
From this view, we see that 43% of ENISA's total budget is allocated to salaries, 28% to operational expenditure, and 29% to overhead (see Figure 3). The percentages are only marginally different for expenditures directly allocated to the work streams.

Figure 3: Fraction of budget allocated to salaries, operational expenditure, and overhead



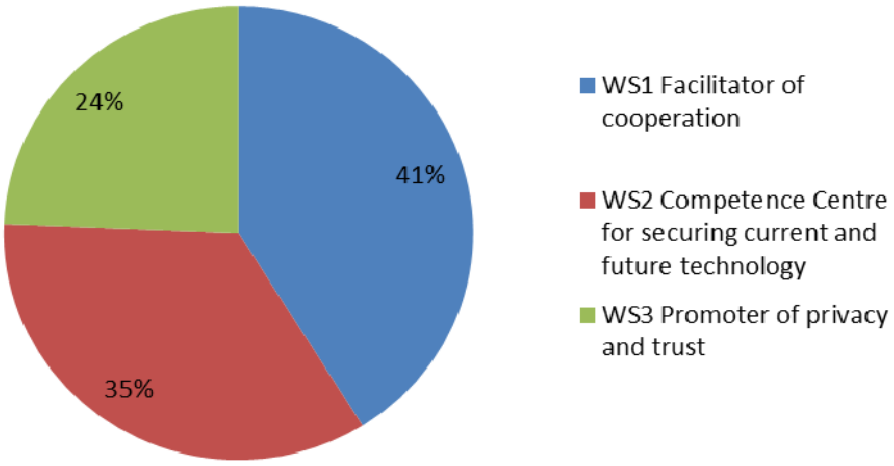
We also observe that 23%, 19% and 13% of ENISA's total budget correspond respectively to Work Streams 1, 2, and 3, i.e. to actual project work (see Figure 3). These expenditures include Title 1, 2 and 3 expenditures, thus covering not only salaries but also administrative overheads and operational expense. 55% of budget is allocated to the work streams in total; however, this does not mean that all of the remainder is overhead. Many of the remaining functions contribute directly to ENISA's mission.

Figure 4: Activity Based Budgeting (ABB) allocation of total cost in ENISA's 2011 budget



Among the work streams, the allocation to WS1 is somewhat higher (41%) than that to WS2 (35%) or WS3 (24%) (see Figure 5). Only cost that is allocated to a work stream is reflected here.

Figure 5: ABB allocation of relevant total cost among the work streams



3.3. Assessments

This section deals with the various assessments of ENISA that have been undertaken, beginning with the evaluation by an Expert Panel, led by IDC EMEA, that was conducted in 2007 (Section 3.3.1). In 2009, ENISA retained Deloitte to conduct a survey of take-up of ENISA deliverables in the Member States, as a successor to an earlier study by GNKS (Sections 3.3.1, 3.3.2). Finally, Section 3.3.3 provides our own assessment of ENISA's performance, based on the available literature, our stakeholder interviews, the European Parliament's mini-hearing of 26 May 2011, and our two site visits to ENISA in Heraklion.

3.3.1. The Expert Panel / IDC 2007 evaluation report on ENISA

As required under the Regulation that established ENISA, the Commission arranged for an independent evaluation of the agency in 2006, which was published in 2007.[76] The report found that ENISA had already reached significant achievements, but that it was clearly not fulfilling its potential.

The report identified numerous serious challenges, including (1) ambiguities in the agency's mission, (2) high and varying expectations among stakeholders (especially in terms of differences between large Member States, who had well established cyber security organisations, in comparison with the newer Member States, who did not), (3) cumbersome management arrangements and a Management Board (MB) too deeply involved in day to day decisions, (4) too few staff relative to the mission, (5) too many administrative staff relative to too few operational employees, (6) rigid staff structure, (7) excessive focus on products rather than outcomes, (8) a location that severely hinders interaction with stakeholders and impacts recruiting and retention, (9) generally weak links to European industry and to the European standards process, and (10) low visibility overall.

As noted in the Introduction to this report, we consider the concerns that were raised to reflect an accurate picture of the agency in 2007. The points made are well substantiated in the report. Stakeholders whom we have interviewed have not contested any of the findings.

3.3.1.1. The issues raised

In 2007, the agency had been in place for only a short time; nonetheless, this report should have raised several yellow flags, and a few red ones.

A few of the concerns warrant further elaboration.

The Management Board was felt to be (1) large to the point of being unwieldy; (2) contentious both internally and with the Executive Director and staff; and (3) too much involved in day to day management of ENISA.

As regards links to industry and standards bodies, the Expert Panel contacted representatives of "… 16 of the main ICT industries, who are considered key actors in the NIS field. … These actors knew about the existence of ENISA but considered its role as very policy-oriented, beyond their immediate interests and not particularly relevant for their activities. These stakeholders consider that European coordination is very important for operational issues such as products standardisation and certification, but have the impression that ENISA is not involved with these issues. They have little interest in promoting a NIS culture in a general sense, nor do they think that it is a priority for the EU

[76] Evaluation of the European Network and Information Security Agency: Final Report by the Experts Panel, IDC EMEA, 8 January 2007
http://ec.europa.eu/dgs/information_society/evaluation/studies/s2006_enisa/index_en.htm.

security market. … The external stakeholders better informed about ENISA had seen its documents and heard its conference presentations, which were defined as good or adequate. However some of them expressed regret that the Agency is not proactive enough beyond the institutional circle of public actors, either through better dissemination and communication or by involving more actively the industry actors."

As regards the agency's location, the report notes: "The location of ENISA in the island of Crete, chosen by the Greek Government, is undeniably remote, 2400 KM away from Bruxelles. The problem is not distance by itself, but its impact on the mission of the Agency which requires continuous interaction with main IT Security policy and research centres. Heraklion is not a capital city, is very far from the main knowledge centers of the security environment, and has limited flights schedules with travel time to reach other EU cities ranging between 7 to 10 hours. Daily trips are almost impossible and attendance to conferences or other events requires at least two or three days."

In terms of recruitment and retention, the report notes that the "… location affects negatively human resources management as follows:

- It limits the pool of available resources for recruitment, because of the lack of European schools for children beyond primary level, the lack of work opportunity for spouses, the lack of an international environment and services under the standards usually enjoyed by the community of international organisations employees. Moreover, the Greek Government has not maintained all promises, which included the establishment of European schools and others advantages for the Agency staff.
- It affects the well-being of the staff creating a turnover problem, as some employees have not been able to adapt to the local conditions. To give an example, there is no theatre and the two cinemas only run movies in Greek. Attracting and maintaining highly skilled people would require a mix of more favourable economic conditions and strong support packages which the Agency has not been able to offer so far."

As regards the high percentage of administrative personnel, European agencies tend to have a high administrative burden whether they are small or large. At the Parliamentary mini-hearing on 26 May 2011, Mr. O'Shea of the Court of Auditors noted that their preliminary finding for this year's report on ENISA determined that ENISA's administrative overhead was some 37%; however, this is not out of line in his view for European agencies of ENISA's size (see also Section 4.2.4).

3.3.1.2. The recommendations made by the evaluation report

Key recommendations of the 2007 evaluation included:

- Renewal of the agency's mandate, and revision of its charter to address ambiguities.
- Post-2009, the "…Agency's size and resources should be increased to reach the critical mass necessary to act effectively and allow for an appropriate mix of skills …"
- The creation of a strategic roadmap for the agency, together with "a multi-annual rolling action plan, including a realistic assessment of potential impacts and measurable success/failure indicators linked with the substantial objectives of the Agency."
- Increased efforts to "… upgrade the marketing communication activities of the Agency in order to improve its visibility to well-identified targets on the basis of a clear and focused message of its role and its activities."
- Changes in management structure and processes so as to increase the ratio of operational staff to administrative staff, and to increase flexibility.

- Measures should be considered to mitigate the operational and economic burdens associated with the agency's location, including increased use of telecommuting and "…the possibility to open a small liaison office in Bruxelles or another network hub city".
- Consideration of a range of possible measures intended to mitigate "…the negative consequences of the location on personnel recruitment and maintenance".

The Panel also recommended "…that the feasibility of moving the location of the Agency from Heraklion be seriously considered, moving the headquarters to Athens or to another EU city with an international environment and greater proximity to the security environment main knowledge centres." This controversial recommendation likely had the effect of diverting attention from many other aspects of the study. We note in any case that the location of the agency is not within our terms of reference for the present study.

3.3.2. The 2009 assessment of ENISA's deliverables

In 2009, an assessment of ENISA's deliverables was conducted by Deloitte on behalf of ENISA.[77] ENISA asserts that it "… did not influence the results of the survey and only ensured that the survey was executed in an independent and objective manner by Deloitte."[78]

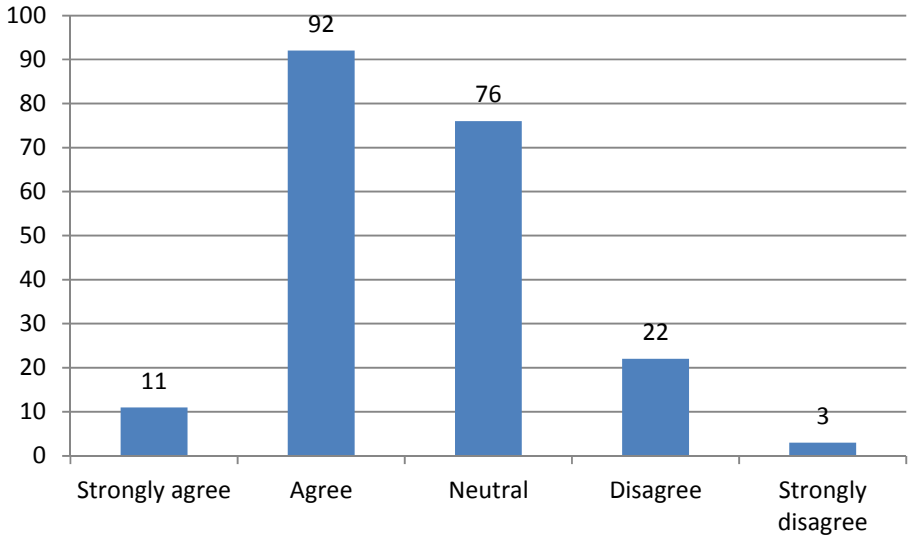
Surprisingly, none of our staff, MB, or PSG interviewees were familiar with the document.

The document represents an online survey of 625 stakeholders. In any survey of this type, there is substantial risk of bias because survey respondents are self-selected. In this case, ENISA stakeholders received multiple email reminders inviting them to respond, possibly magnifying selection bias effects.[79] This is not a methodological complaint, it is a common and perhaps unavoidable problem with online surveys, but nonetheless the survey results should be interpreted with caution because survey respondents will tend in many cases to be more aware of the agency and perhaps more friendly to it (or possibly more hostile to it) than would be expected in a random sample.

The document purports to address uptake of deliverables, but nonetheless seems to continue to reflect the predisposition noted in the 2007 evaluation to focus on the product that is delivered rather than the effects that it has. Even so, a few of the findings of the study should have raised yellow flags if not red. In terms of conference attendance, for example, consider Figure 6. Taking into account (1) the previously noted selection and pre-selection biases, and (2) the fact that responses were dropped from the survey unless they responded to the full questionnaire, then the high number of "neutral" responses (to this question and to most about ENISA participation at events) might well indicate that even those most favourable to ENISA were not always convinced that the outputs had value to them.

[77] "Measuring uptake of ENISA deliverables in the Member States," available on the ENISA web site.
[78] Page 2.
[79] See page 14 of the report.

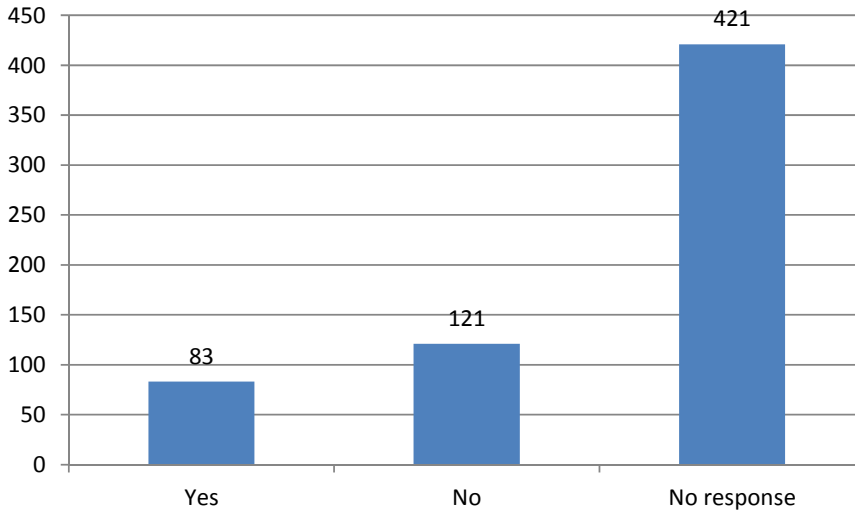
Figure 6: Number of respondents who agreed that ENISA participation at events was adequate



Source: Deloitte

As another pertinent example, Figure 7 shows that nearly 50% more stakeholders (121 versus 83) felt that ENISA presentations did *not* enable them to take practical actions as those who felt that they did, while more than two thirds of the respondents declined to answer the question at all. In terms of the concrete utility of ENISA presentation activities as they were conducted in 2009, and bearing in mind once again the biases inherent in such a survey, this should raise concerns. This finding is consistent with the results of a similar study conducted for ENISA by GNKS two years earlier, which found that "… notwithstanding their overall quality, the deliverables have not acted as an instrument of change of current public policy or operational activities in the field of information and network security activities."[80]

Figure 7: Number of stakeholders who felt that ENISA presentations enabled them to take practical actions



Source: Deloitte

[80] GNKS, The practical use of ENISA's deliverables in member states, January 2008, available from GNKS.

3.3.3. Our assessment

This section of the report provides our assessment of ENISA's operation today. It is positive rather than normative – that is, it describes ENISA as it is, not as it ought to be. To the extent that they constitute challenges or problems, the issues that are assessed here re-emerge in Chapter 4, which considers possible ways forward.

In terms of assessing the effectiveness and efficiency of ENISA in its present form, the best starting point – in many respects the only reliable starting point – is the 2007 evaluation.

The 2007 evaluation may be the starting point, but we are pleased to report that it is not the end of the story. A key turning point for the better for the agency appears to have come with the appointment of Dr. Udo Helmbrecht as Executive Director in October, 2009. Dr. Helmbrecht, who previously headed the German Federal Office for Information Security (known as the *Bundesamt für Sicherheit in der Informationstechnik*, or *BSI*) combines in a single individual subject matter with expertise in NIS, experience running an agency some eight times larger than ENISA, and a global professional reputation.[81] Dr. Helmbrecht has an open, pragmatic management style, and the willingness and ability to take on the challenges of the agency. He has built a solid management team, drawing both on those who were already working at ENISA and on new hires. Our sense is that staff are working together as a team and achieving results.

ENISA is running visibly better than it did in 2007 or 2009, and in a great many respects. Among the concerns raised in the 2007 evaluation that were within the remit of ENISA to fix, nearly all show concrete signs of improvement.

Many of the concerns raised in 2007 that depend on action at European level have, however, scarcely been touched.

We emphasise that our assessment does not constitute a formal evaluation. The study does not entail the resources or time frame that would normally be associated with an evaluation, and a formal evaluation is not included in our terms of reference. The practical reality is, however, that in light of the extension of ENISA's charter, no independent evaluation has been undertaken since 2007. We could not put recommendations forward without first establishing a clear baseline as to the state of ENISA today.

In this section of the report, we first consider in turn the concerns that were raised in the 2007 evaluation, starting with ambiguities in the agency's mission (Section 3.3.3.1) and progressing to low visibility overall (Section 3.3.3.10). These challenges relate to ENISA's mission as it existed in 2007 – the subsequent expansion of its mission, and the further expansion that is likely to be needed in years to come, raise additional issues. We consider these issues in the remainder of this section.

3.3.3.1. Ambiguities in the agency's mission

In principle, ambiguities in ENISA's mission can only be addressed at European level, not by the agency itself. This has not happened. Regulation 1007/2008, which extended ENISA's mandate to 2012, did nothing to change or clarify its responsibilities (or anything else for that matter).

[81] Hiring Dr. Helmbrecht could be said to respond to a recommendation from the 2007 evaluation: "The reputation and the visibility of ENISA, and probably its potential impacts, would be greatly helped by the presence of a high-profile figure well recognised in the security environment, acting as an ambassador and a reference point for the Agency. It is possible that such a figure would not be interested in the day-to-day management of the Agency." Dr. Helmbrecht is the rare individual who has both technical and management skills and interests.

In its response to the 2007 evaluation, the Management Board (MB) requested revisions to the goals and tasks expressed in the 2004 Regulation that establishes ENISA.[82] They specifically called for merging Article 2 (objectives) with Article 3 (tasks) "… to set outcome-based key objectives that are realistic and within the scope of the Agency." We share the MB's interest in identifying and monitoring outcome-based critical performance indicators (see Section 3.3.3.7), but are not convinced that modifying the Regulation to combine and possibly conflate objectives with tasks is the most appropriate way to get there.

Pending any actions at European level, the MB sought in its response to the 2007 evaluation to clarify its criteria in responding to requests for advice and/or assistance:

The Board believes that requests should always meet the following criteria:

- They should clearly fall within the Agency's stated aims and priorities;
- They should be submitted in time to allow them to be taken forward in the following year's work programme (except for the rare circumstance of something being time critical);
- They should benefit Europe as a whole or, as a minimum, more than one Member State.

In addition, requests could be accepted if they meet the following criteria:

- They should contribute to the European Institutions' agenda for the information society (such as requests from the Commission to support legislative or administrative developments);

and/or

- They should provide opportunities for the Agency to participate in the practical implementation of guidance it has issued.

Our perception is that mission ambiguities are less of a problem than they were in 2007, but the confusion has not gone away.

3.3.3.2. High and varying expectations among stakeholders

The 2007 evaluation noted large disagreements, especially in terms of differences between large Member States (which had well established cyber security organisations, and in some cases a moderately well-developed domestic NIS industry) in comparison with the newer Member States (who did not). Among the former group, there were concerns that an overly active ENISA might get in the way; among the latter group, by contrast, there was a desire for ENISA to help more actively.

Today, some stakeholders suggest that this has become less of an issue. Perhaps the process whereby ENISA staff and the MB and PSG work out priorities is addressing this need. In any case, the issue can largely be viewed today as having been subsumed within ambiguities regarding ENISA's mission (see Section 3.3.3.1) and challenges within the Management Board (see Section 3.3.3.3).

[82] See the minutes of the MB at http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1/decision_09.pdf.

3.3.3.3. Cumbersome management arrangements and a Management Board (MB) too deeply involved in day to day decisions

Interviewees among ENISA staff and the MB both confirm (1) that the relationship between the MB and the Executive Director (ED) was strained in the past, and (2) that interactions are greatly improved today, largely as a result of the current ED's open style and willingness to consider the views of others. An MB interviewee also claims that interactions *within* the MB, while still contentious, are far less so than in the past.

The process of formulating ENISA's work programme for 2012 is both a major cause and an index of the improved relations between the agency and the MB. In previous years, the work programme was prepared by ENISA staff, with no meaningful opportunity for the MB (or the PSG for that matter) to provide early, strategic input. The complete proposal was then presented to the MB for approval at the end of the process. This year, by contrast, ENISA staff came to the MB and PSG at the very beginning of the process and invited their input on all aspects of the 2012 work programme. This was a much more inclusive process that much more effectively drew on the skills and competencies of the MB and the PSG. All interviewees (staff, MB and PSG) welcomed this change enthusiastically.

As noted in Section 3.2.2, the MB consists of 36 individuals. This is far larger group than is consistent with the efficient functioning of a Management Board for a European decentralised agency.[83]

The 2007 evaluation also notes that: "The size of the MB and its extensive powers on the Agency make for a difficult governance. The MB must oversee much of the administrative activities of the Agency, and this creates frustration in such a large assembly which would be better suited to strategic level discussions and decision making."

As regards the size of the MB, it is perhaps worth noting the comments of the evaluation of decentralised agencies in the EU:[84] "In the majority of cases, the composition of the management boards does not fully balance the interests needing to be taken into account. In particular, there is a tendency to include full representation of all Member States, although it may not be necessary. This often occurs at the expense of the representation of other more relevant stakeholders. In a few instances, an imbalance in the forces of some players entails blockages or inefficiencies. Overall, the evaluation team concludes that the standard approach is unnecessary, costly, and ineffective. There are interesting exceptions to the dominant model of agency governance, for instance in the case of EFSA having a 15 member board mainly composed of professionals and experts. Such cases may to some extent be considered as pilots for future reforms and at a minimum deserve consideration."

It is abundantly clear that if ENISA were a new commercial entity, and if its Management Board were being designed from the ground up, one should not choose to structure the MB as ENISA's MB is currently structured. There should be no need for an MB nearly as large as the organisation as a whole.

On the other hand, we have to note that we interviewed multiple MB members, and all were of the view that the MB functions well enough, all considered, in light of its responsibilities. The things that have to get done, get done.

---

[83] See Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, at: http://ec.europa.eu/dgs/secretariat_general/evaluation/docs/decentralised_agencies_2009_part1_en.pdf.

[84] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, op. cit.

Reviewing the MB minutes in detail, we found a number of things that might possibly suggest some degree of dysfunction in the MB. There are things in the record that might suggest that the MB has trouble coming to grips with difficult issues. In one instance, a number of issues were spun off to a committee, but we find no indication of any real follow-up.[85] In another instance, the minutes show that an "outsourced study about the impact of increasing the staff working for ENISA" was commissioned, but the completed study never appears in minutes (or anywhere else for that matter, so far as we have been able to determine to date).[86] In yet another instance, we learn in the course of a difficult discussion over the Greek government's apparently unsolicited offer to make office space in Athens available to ENISA that the Executive Director had commissioned work by Deloitte to study how to use the space. We have located that study, and a similar one on the same subject by Ramboll, but we find no indication that they ever surfaced in the MB. None of these observations is dispositive, but we take them collectively as possibly suggesting that there might be some issues with the way the MB operates.

The 2007 evaluation recommended delegation of any day to day administrative powers to a smaller standing committee. This has not been done. In its response to the 2007 evaluation, the MB noted: "The Board considered whether the participation of all Member States of the European Union on the Board made it unwieldy as a decision making body. This was not considered a real problem in practice. … The Board could, and has, appointed smaller groups of individual Board Members to carry out specific tasks and this provided opportunities to meet Board objectives more economically." We should add that an MB interviewee felt that "any tensions within the MB will not necessarily be easier to manage in a small group than in a large one."

Review of MB minutes indicates that the creation of an Executive Committee was discussed, but foundered because (1) many MB members were unwilling to be excluded from the Committee, and (2) many feared that the Executive Committee would effectively supplant the MB, and that MB members who were not members of the Executive Committee would be excluded from information and from decisions.[87]

Alternatively, there might be value in establishing a clearer boundary between the functions of the MB and those of ENISA staff, so as to enable the former to concentrate on strategic issues, as they should. This could either be done in a revised Regulation, or by the MB under its own authority. Doing so would respond to a recommendation of the 2007 evaluation, which felt that the MB was too much involved in day to day activities. It had also been a recommendation of the "MB subgroup on future orientations", chaired by Mr. Smith of the UK.[88] One interviewee suggested that "…it would probably help the functioning of Agencies and their Boards if the Commission produced guidance on the role of the Board and the role and responsibility of Board Members individually and collectively".

At the same time, our interviews strongly suggest that many of the problems identified in the 2007 evaluation were the result of a uniquely strained relationship between the MB and the then-current Executive Director (ED). Numerous interviews suggest that the ED did not

[85] See the minutes of MB meeting 14 (October 2008), "Report of the MB subgroup on future orientations". It notes that the chair of an internal subgroup "… expressed the concern of the sub group regarding the preparation of the Board for the new management of the Agency. He highlighted that a clear distinction of the powers of the MB and the ED should exist. He suggested the preparation of a paper describing the relation between the MB, the ED and the Stakeholders. A draft of that paper will be distributed in the forthcoming MB meeting …".

[86] See the minutes of MB meeting 12 (October 2008).

[87] See the minutes of MB meeting 9 (January 2007), and especially of MB meeting 12 (March 2008).

[88] See the minutes of MB meeting 14 (October 2008), where Smith notes that "… a clear distinction of the powers of the MB and the ED should exist. He suggested the preparation of a paper describing the relation between the MB, the ED and the Stakeholders."

enjoy the confidence of the MB. One interviewee indicated that the former ED contended that the MB had no role in regard to overall staff planning, based on his (overly literal in our view) reading of Article 7 of the 2004 Regulation, which says that the Executive Director is responsible for "all staff matters".[89] We think that the only reasonable way to read the 2004 Regulation is to say that, while day to day staff management *must* be the province of the ED, that the MB clearly has a role to play in staff planning at a strategic level. Indeed, this is how the matter was eventually resolved, with the ED submitting a multi-annual Staff Policy Plan (SPP) to the MB for its approval.

Recommendation 2. Clarify the overall mission of the MB.

Any revision of the ENISA Regulation should state affirmatively what the mission of the MB is, and clarify its role relative to that of the Executive Director.

This does not necessarily imply a changed role, but rather a clearer expression of the MB's role.

Recommendation 3. Clarify the MB's role in staff planning.

Any revision of the ENISA Regulation should formalise the MB's role in strategic staff planning.

Since this is largely a clarification of existing arrangements, it does not represent a change that is relevant to the impact assessment that appears in Section 5; however, given that this has already been a source of confusion and contention, it is appropriate to make it an explicit recommendation for this report. Note that it is entirely consistent with Article 5(9) of the Commission's proposed Regulation: "The Management Board may adopt the Multi-Annual Staff Policy Plan, after consulting the Commission services and having duly informed the Budgetary Authority."

Based on the early history of ENISA, another issue needs to be considered. The MB became embroiled in a complicated dispute, the details of which are not relevant here. MB members felt the need to understand their individual legal liability, but did not consider it appropriate to rely on ENISA's legal resources for an opinion. The MB did not have, or did not believe it had, the ability to retain its own expert advice.

This is reflected in our interview results. Two interviewees noted a need to explicitly make legal resources directly available to the MB. One wrote that "… the Board lacks access to independent legal advice on those staff matters that can involve the Board." The MB can be subject to different legal needs than those of the agency, including questions regarding the legal liability of MB members for actions taken or not taken.

Under normal circumstances, legal resources and other staff resources available to the agency can also support the MB; however, in rare or exceptional instances, the use of agency resources is inappropriate. There could be issues of confidentiality, privacy, or conflict of interest. More generally, the interests of the agency are not necessarily aligned in all cases with those of the MB or its members.

[89] See also the minutes of MB meeting 14 (October 2008): "The Chair emphasized the need for an overview of the agency's staff before the discussion of the Work Programme 2009 will take place. He expressed his dissatisfaction about the absence of an agency's staff policy plan for 2009-2011 and asked the ED to inform the Board regularly about the changes in the allocation of staff as this has budgetary implications."

This need is not limited to actual court cases. There could also be a need to determine whether a claim has merit. This could entail significant legal and factual research.

ENISA experienced such a problem in its early years. So far as we can see, problems of this type will come up only rarely, but there is no reason why they could not come up in any of the decentralised agencies. In the case that arose at ENISA, the Commission took appropriate action, in our view, despite the lack of a clear mandate.

A wealth of support is available to the Commission and to the Parliament for their own activities. The degree to which these facilities are available and appropriate for use by the Management Board of a decentralised agency (whose members are not employees) is not clear to us; if any *are* available, their use is certainly not understood. We think that a bit of thought in order to craft a more general mechanism and to make the MBs of decentralised agencies aware of it[90] is warranted.

Recommendation 4. Ensure that the MB has access to independent legal advice.

Ensure that the MB has access to independent legal and staff resources when required, especially in regard to personnel matters. Consider making similar support available to all of the decentralised agencies.

This recommendation would appear to be consistent with one of the Commission's goals in the proposed regulation: "The Management Board is also given adequate resources in case it needs to take executive decisions and implement them (e.g., if a staff member lodges a complaint against the Executive Director or the Board itself)."[91]

3.3.3.4. Too few staff relative to the mission

The 2007 evaluation called for increasing the staff size of ENISA to not less than 100. Many of the responses to the Commission's 2007 consultation called for a substantial increase in staff size. These proposals were based on the agency's mission at the time, and thus do not take into account the expansion in responsibilities that has taken place since, to say nothing of the further expansion in responsibilities that is likely in the coming years.

At the time of the 2007 evaluation, ENISA had 52 headcount allocated (including 8 detached national experts). Six of these slots were not filled. Today, ENISA has 57 total headcount allocated, and there are only transient vacancies. There has been a growth of 5 in the allocated headcount, and an effective growth nearly twice that due to the elimination of vacancies; nonetheless, staff size remains far below what was recommended at the time, and probably well below what is efficient for a European agency.

A survey of the MB conducted as part of a 2009 study of decentralised European agencies suggests continued concerns over the adequacy of ENISA's staffing. "In the management board survey, there is considerable disagreement about whether the agency addresses the needs it was set up to address: Only 50% agree, while more than a third (36%) disagree or strongly disagree (14% neither agree nor disagree). While we cannot know for sure what lies behind these figures, the answers to another question

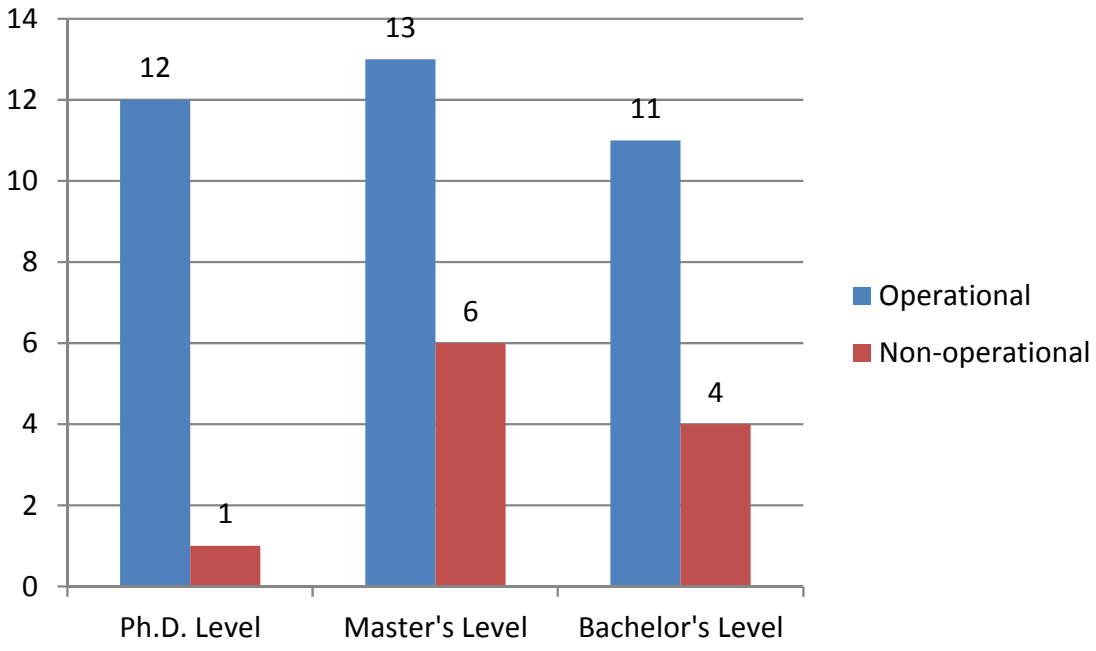
[90] The concerns were prompted in this case by issues of individual liability of MB members, but in our view any support should be managed by the MB as an entity, not by individual members.

may provide a clue: when asked which factors have a negative influence on the agency, the two factors most frequently pointed to were "insufficient financial resources" and "insufficient human resources" (both indicated by 10 of the 14 respondents)."[92] An alternative interpretation is that the diverging views on the adequacy of staff size are simply a reflection of divergent visions of ENISA's proper mission (see Sections 3.3.3.1 and 3.3.3.2).

Indeed, since ENISA has not undertaken operational functions to date, it is difficult to say what the "correct" staff size should be. A less-than-optimal staff size implies that things that are worth doing will not be done; however, it is impossible to point to a particular critical operational activity that will not be done if staff size falls below some critical threshold.

Staff quality is as important as staff quantity. Academic qualifications represent one measurable element of staff quality. Figure 8 denotes the level of the highest degree attained by each staff member. More than two thirds of the operational staff hold at least one advanced degree (Master's or Ph.D. level).

Figure 8: Highest degree attained by staff



Source: Study team, based on information provided by ENISA[93]

ENISA reports that the five Programme Managers (typically at AD8 and AD9 levels) typically have at least ten to twelve years of relevant experience. More junior staff may have less experience, but even an AD6 post requires at least three or four years of relevant experience.

ENISA has a number of strengths in terms of staff capacity. Consistent with the data on academic preparation and with years of experience, our perception is that ENISA staff are

[91] Page 9.

[92] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009.

[93] This reflects a snapshot of the 59 employees and Seconded National Experts (all of whom have degrees) who were on ENISA staff in June 2011. At that time, 47 staff members had a degree, 12 staff members did not.

viewed as being competent. There has also been an effective increase in the operational headcount through improvement in the ratio of operational employees to administrative employees (see Section 3.3.3.5). These combined strengths appear, however, to fall short of producing the total number of operational staff that the agency would need to fully accomplish what many would like to see it achieve.

3.3.3.5. Too many administrative staff relative to too few operational employees

The large weight of administrative staff has been an issue for ENISA from the beginning, and continues to be an issue; however, there have been concrete improvements.

Before discussing the improvements, we should note that ENISA faces two substantial challenges. The first is that as a small European agency, it has an inherently high administrative burden in comparison to its total staff size. The second is that the complex travel arrangements necessitated by ENISA's Heraklion location require, according to ENISA, three full time administrative staff solely to deal with travel arrangements.

The challenge of high relative administrative costs relative to small staff size is by no means unique to ENISA; rather it is common to European decentralised agencies. A study of the effectiveness of decentralised European agencies found: "The evaluation has identified a series of factors affecting external efficiency, i.e. achieving good results and impacts at low cost. Of these, administrative tasks are by far the most significant. On average, they consume about one-third of the agencies' staff resources, although variations between agencies are substantial, with figures ranging from 14% to 54%. Smaller agencies are at a significant disadvantage since the regulations and procedures with which the agencies have to comply are largely the same regardless of the agency's size. It seems that in order to operate efficiently, an agency needs to reach a certain critical size. The data indicates that this critical size lies somewhere between 50 and 100 staff." Indeed, Table 2 (from the same Ramboll study, based on data provided by the European Court of Auditors) clearly demonstrates that ENISA is squarely in line with its peer group of decentralised European agencies.

This finding is entirely consistent with the remarks of Eoin O'Shea of the Court of Auditors at the Parliamentary mini-hearing of 26 May 2011, in observing that ENISA's 2010 overhead of 37% is consistent with that of other decentralised agencies of its size.

Table 2: Relationship between the size of a decentralised agency and the share of administrative staff

Size (number of staff)	Share of administrative staff	No. of agencies	Names of agencies
Large (>150)	28%	7	Cdt, EASA, EAR, EFSA, EMEA, EUROJUST, CHIM
Medium (75-150)	33%	9	CEDEFOP, ECDC, EEA, EMCDDA, EMSA, ERA, ETF, EUROFOUND, FRONEX
Small (<75)	37%	5	CPVO, ENISA, EU-OSHA, FRA, GSA
Overall	**30%**	**21**	

Source: Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, Part 2, page 96, based on data from the European Court of Auditors' annual specific reports on individual agencies – Year 2007 (except EMSA and OHIM 2006) – Categories and calculation (weighted average)

As noted, improvements over time were needed in order to reach these levels. At the time of the 2007 evaluation, the agency included a central management department with a staff of 10 under the ED.[94] Eight of these staff were reassigned internally to departments with more clearly defined operational functions.

There have also been efforts to re-train administrative personnel to enable them to undertake operational tasks. These efforts, however, have faced significant practical hurdles, and have apparently met with only mixed success.

In our view, the high fraction of resources devoted to administrative staff continues to be an issue to the extent that it reinforces the concern that ENISA's staff size is too small. It is a problem, but it is a problem that is common to decentralised agencies the size of ENISA. The implicit concern that ENISA's staff arrangements were inefficient, as evidenced by a high ratio of administrative staff to total staff, appears to have been well founded in 2007. Today, ENISA is on a par with its peer group of small decentralised agencies in terms of the ratio of administrative staff to total staff, despite a high administrative load to manage travel arrangements.

3.3.3.6. Rigid staff structure

In 2007, ENISA's technical staff was split among multiple departments. Today, there is a single operations group of 35 staff, under a single manager. Project oriented teams can be created or broken up as needed, with the individuals reassigned within the group when no longer needed. There are currently five Programme Managers who manage teams of from two to eight experts in terms of subject matter, but apparently not in regard to personnel matters.

In the abstract, this solution may not be ideal – one interviewee suggested that the lack of a second level management structure for personnel matters in such a large group might mean that some personnel issues are not dealt with as promptly as they should be. The agency recently appointed a deputy for the group that does operations, which should help.

All things considered, the problem identified in the 2007 evaluation seems to be much less of a concern today than it was at the time.

A remaining staff flexibility issue relates to changing needs for detailed skills in the staff. As skill needs change over time (due to changes in technology, or changes in the nature of threats), ENISA may be less able than it ought to be to respond to the changing environment with a changing skill mix. First, the location introduces challenges in recruiting top talent with highly specialised skills that are highly valued in the commercial marketplace (see Section 3.3.3.8). Second, European personnel rules may make it difficult to reassign skilled workers whose skill profiles no longer match ENISA's needs.

3.3.3.7. Excessive focus on products rather than outcomes

In developing the work programme for 2012, outcome-oriented performance indicators (KPIs) were developed in addition to deliverable-oriented KPIs. ENISA staff observed, rightly in our view, that each has its place. The outcome-oriented KPIs are valuable for strategic planning, but it may be possible to properly assess them only years after the fact. Conversely, deliverable-oriented KPIs are more or less immediately measureable, but they indicate only that the deliverable was produced, not necessarily that it had the desired effect.

[94] See pages 47 and 48 of the 2007 evaluation report.

It is not at all unusual for a European programme to have difficulty in providing hard, quantitative measures of its effectiveness. A study of the effectiveness of decentralised European agencies found: "Adequate monitoring is the basic requirement for being able to carry out the other oversight activities in a way that lives up to the requirements. However, monitoring is not very well developed in terms of the use of quantifiable objectives and indicators. All agencies monitor their use of resources and most monitor output in some way. Several agencies are making an effort to develop results-based performance indicators, usually connected to their activity-based management systems. However, actual use of such indicators is still extremely rare, meaning that the monitoring of results and impacts is almost non-existent. Thus, the monitoring activities share the basic flaw of the evaluation practice: that real effectiveness cannot be (is not) assessed, which means that the contribution of monitoring activities towards improving performance is, at best, only applied to outputs and internal efficiency, and not results. This is carried directly over into the reporting activities, which almost never go beyond outputs and the use of resources because the monitoring activities do not produce the full range of data required to live up to the requirements of the framework Financial Regulation."[95]

On the other hand, the same report went on to note: "The use of impact indicators in the new work programme and the annual report for 2008 is quite advanced compared to other agencies. ENISA is one of very few agencies that has succeeded in defining a number of impact-oriented indicators rather than only output indicators in their monitoring and reporting. This may be considered best practice."[96]

There has been substantial progress, but our sense is that hard, systematic attention is still needed over time.

3.3.3.8. A location that severely hinders interaction with stakeholders and impacts recruiting and retention

As noted in the introduction, the location of the agency is not part of this study's terms of reference; however, it is quite impossible to meaningfully discuss the agency's budget or staffing without considering the effects of its relatively remote location in Heraklion, Crete.

This is a common problem for independent agencies, and is not unique to ENISA. A comparison among decentralised European agencies found: "The location cost also affects efficiency to a significant extent, again with considerable differences between agencies. Less accessible locations, in terms of travel cost and time, affect both the resources needed for achieving results and the results themselves, especially where agencies' activities require extensive networking."[97] The effect on ENISA is particularly dramatic because (1) coordination, including the need for physical, is central to ENISA's mission; (2) ENISA is remote not only in terms of distance, but also in terms of connections (which are far worse in winter than in summer); and (3) ENISA is heavily dependent on recruiting cyber security experts whose skills are heavily in demand by industry in locations that are less remote.

The location has two main effects: (1) it reduces the efficiency of travel on the part of ENISA staff (see Section 3.3.3.8.1), and (2) it introduces challenges in terms of recruiting and retention /see Section 3.3.3.8.2).

[95] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009.

[96] Ibid., Part 3, pp. 135-136.

[97] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009. The report goes on to note that host country subsidies of rental costs, as in the case of ENISA, may partially offset these inefficiencies.

In considering the effects of ENISA's location, one should not forget that there are also positive aspects. Heraklion has both beauty and charm. We also note that the Greek government has been generous in their support of ENISA, providing free rent to the agency for its main location in Heraklion and also for a satellite office in Athens that is used for meetings of the ENISA Management Board (MB) and the ENISA Permanent Stakeholders' Group (PSG). The proximity to FORTH, a respected research institution, also provides some synergies.

3.3.3.8.1 Travel inefficiencies

In understanding the impact of travel, it is important to remember ENISA's function and mission. Very little of ENISA's mission is operational. As previously noted, ENISA's primary functions involve serving as a centre of expertise, coordination, and dissemination of best practice.

At the European Parliament's mini-hearing on 26 May 2011, Mr. Jarkko Saarimäki of the Finnish CERT noted succinctly that this coordination function cannot be done remotely – at least, not initially. A great deal depends on building trust, which has to be accomplished face to face. Email, teleconferencing and electronic tools have their place, but physical travel is absolutely critical to the effective accomplishment of ENISA's mission.[98]

The ease or difficulty of travel to Heraklion varies based on many factors. During the vacation season, it can be fairly easy to find direct, inexpensive flights from certain airports, but typically only Friday through Monday. During the winter, service is limited and usually requires a transfer in Athens, with substantial loss of time.

Among decentralised European agencies, ENISA is not unique in this regard, but it is clearly among the worst. A study of decentralised European agencies[99] found: "Accessibility is a matter of travel cost and travel time, the latter being affected by the need to have flight connections, the need to stay one or two nights in the agency headquarter city, and the sometimes long taxi drive to the airport. Accessibility is however not needed for all European agencies. In fact, it is mainly desirable where the agency has an intense networking activity, something which occurs where its main activity consists of collecting harmonised information, contributing to the soft coordination between Member States and European Institutions, providing advice to policy-makers through panels or networks of experts, and facilitating operational coordination between Member States." Based on these factors, the study found that six European decentralised agencies had problems due to locations. Among these, ENISA was one of two characterised as have a "serious" accessibility problem.

The same study noted:[100] "Geographically, ENISA is the remotest of all agencies measured in distance from Brussels, and the location in Crete means that ENISA has the highest relative travel cost of all agencies … – in terms of both direct travel costs and time spent on travelling. Given the limited resources, this constitutes a significant burden on the agency's resources."

These challenges have somewhat distinct effects on (1) ENISA staff, (2) MB and PSG members, and (3) outside stakeholders.

---

[98] At the same hearing, Ilias Chantzos of the PSG (and of Symantec) noted that the location of staff makes no difference *for an organisation that is doing incident response* (his emphasis). This does not contradict the need for physical presence for ENISA's coordination function – rather, it reinforces the need.

[99] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009.

Travel expense from Heraklion is certainly a consideration. In 2010, mission expenses for ENISA totalled €547.115, representing an average mission cost of €1,303 per mission over 420 missions. This corresponds to 23% of Title 3 budget appropriations for the year out of €2.354.988, or 7% of total budget appropriations of the year out of €8.113.188.[101]

Travel expense is significant, but even more significant is the loss of time on the part of senior professionals. ENISA reviewed their electronic mission records at our request,[102] and identified 18 "heavy travellers" who travel more than 30 days per year. Their mission days collectively represent 68% of all ENISA mission days. The 18 heavy traveller ENISA staff were away for 908 mission days during the past twelve months (June 2010 through May 2011). This represents an average of 0.97 days per calendar week, not allowing for vacation weeks or sick time weeks. The heavy travellers conducted 287 missions, with estimated efficiency (productive time divided by total mission duration) of 54%. This implies that the average mission has a duration of 3.2 days, of which 1.7 days are productive and 1.5 days are wasted with travel. Obviously, some trips are shorter, while others must be even longer.

For 134 out of 420 missions in year 2010, or 32% of total missions, an overnight in an Athens hotel was required. These overnights contribute both to lost time and to wear and tear on the staff.[103]

63 (23%) of the 287 heavy traveller trips were triangle trips (more than one destination per trip). Triangle trips represent an efficiency gain, because the unproductive Heraklion-Athens flight time is incurred only once to reach more than one mission destination. Achieving 23% triangle trips appears to us to already be at the upper end of any efficiencies that could potentially be gained by combining trips. The benefits of a more efficient triangle travel schedule are already reflected in the estimate of 54% efficiency. We conjecture that infrequent travellers are rarely able to conduct triangle trips.[104]

All in all, the large amount of unproductive travel time and the substantial duration of every mission represent a substantial personal burden on ENISA's heavy traveller staff, and a significant burden on ENISA's operational efficiency.

As for the MB and PSG, their meetings have rarely if ever been conducted in Heraklion in recent years. The MB has met primarily in Athens, sometimes in another Member State, such as the Member State that holds the rotating presidency of the Council. In the past, those meetings were conducted in hotels; more recently, those meetings were held in ENISA office space in Athens that has been donated by the Greek government (thus reducing the financial burden on ENISA). At the same time, these MB and PSG arrangements are not without cost – of the 287 missions undertaken by ENISA heavy travellers in 2010, 57 were to Athens, and many of these presumably in support of MB or PSG meetings.[105]

---

[100] Part 3, page 134.
[101] ENISA, "Note for the attention of Mr Giles Chichester, MEP, Rapporteur on ENISA, ITRE Committee", 6 June 2011.
[102] Ibid.
[103] Ibid.
[104] Ibid.
[105] Ibid.

As for outside stakeholders, ENISA staff indicate that it is quite difficult to get external experts to pay short visits to Heraklion. This is however less of a problem for longer stays in the summer, for example for week-long training workshops.

3.3.3.8.2 Recruiting and retention

At the time of the 2007 evaluation, ENISA had six openings out of 44 staff, and some of these openings had been long-standing. Today, there are only a small and transient number of openings. In fact, ENISA is among the best of European agencies in the speed with which it fills open positions.[106] Why, one might ask, should we worry about recruiting today?

At the time of the 2007 evaluation, ENISA was experiencing high turn-over of professional staff. For the past few years, attrition of staff has been about seven per year, or 12%, which is within normal expectations. Why, one might ask, should we worry about retention today?

As noted in the 2007 study, Heraklion's location complicates recruiting and retention in several different ways. First, the international school that has been put in place may be adequate for grade school children, but there simply are not enough students to create a viable environment today for high school students.[107] In the early years of ENISA, several highly skilled workers left ENISA as soon as their children reached high school age. Today, it is more likely that they will not accept employment in Heraklion in the first place.

At the same time, it must be acknowledged that the Greek government has already made a significant investment in the European School, and continues to persevere in its efforts to expand and improve it, even in the absence of a long term commitment for ENISA to continue to exist. The Greek Government has acknowledged the need for better facilities for the European School, and has started the construction of a new large and state of the art equipped school building, located on land provided by the University of Crete, adjacent to the work premises of ENISA. The new school building will have a capacity of more than 600 pupils. The plan is that it be ready for the school year 2013-2014; however, it is worth noting that the intent had been to make such facilities available to ENISA parents years ago.

Second, if a professional accepts employment at ENISA, it is unlikely that his or her significant other will find suitable employment in the area.[108] Thus, families comprised of two professionals will tend to decline employment.

Third, while Heraklion is beautiful and offers a number of free time activities, the cultural facilities (notably for those who do not speak Greek) are simply not competitive with those that a cybersecurity expert (who typically will be much sought after by industry, with many choices of where to work) could find in a cosmopolitan European capital city.[109]

Taken together, these restrictions mean that ENISA has been successful in hiring a sufficient *number* of staff, but with a significant tendency toward either (1) younger professionals, including singles, and (2) mature professionals whose spouses do not work, and whose children are either away at university or else adults and off on their own. The generation in between is conspicuous by its absence at ENISA, and this

[106] Remarks of Eoin O'Shea of the Court of Auditors at the Parliament's mini-hearing on 26 May 2011.

[107] This implies that, in order to succeed, the European School needs to draw a substantial number of students from the region. ENISA parents alone do not have have enough children of secondary school age.

[108] This is especially true for families that do not speak Greek, but it can sometimes be an issue for families from other cities in Greece.

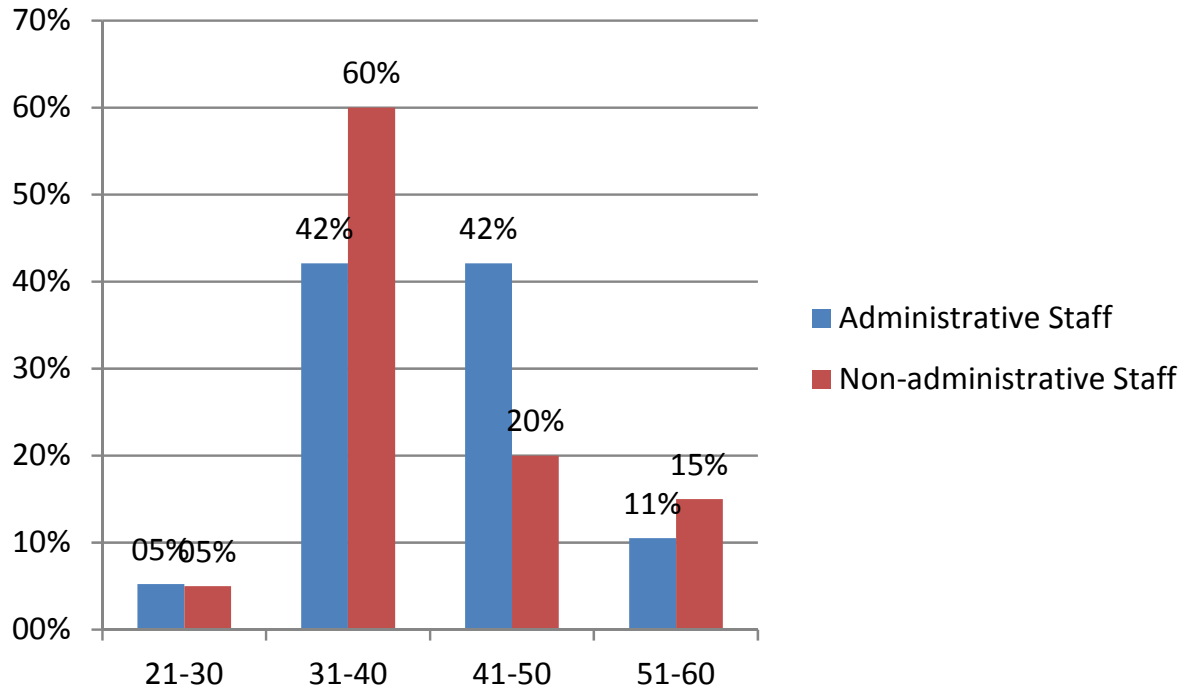
[109] Cf. interview comments quoted in the 2007 evaluation.

means that an important tier of first and second level managers, and senior technical experts, is simply not there.

This difference is clear when one considers the staff composition, as shown inFigure 9, based on data kindly provided by ENISA staff. Approximately half of the 19 administrative staff are Greek (although not necessarily originally from Heraklion). The lack of secondary education in a language other than Greek is probably largely irrelevant to them, and the challenges regarding jobs for the significant other probably less daunting than for those who are not Greek. Most of the 19 administrative staff are in the 31-40 and 41-50 age groups, with just a few in the 21-30 and 51-60 age groups.

By contrast, less than 25% of 39 non-administrative staff are Greek. Thus, schools for children and jobs for the spouse are more of an issue for a majority of non-administrative staff.

Figure 9: Age distribution of administrative and non-administrative staff (%)

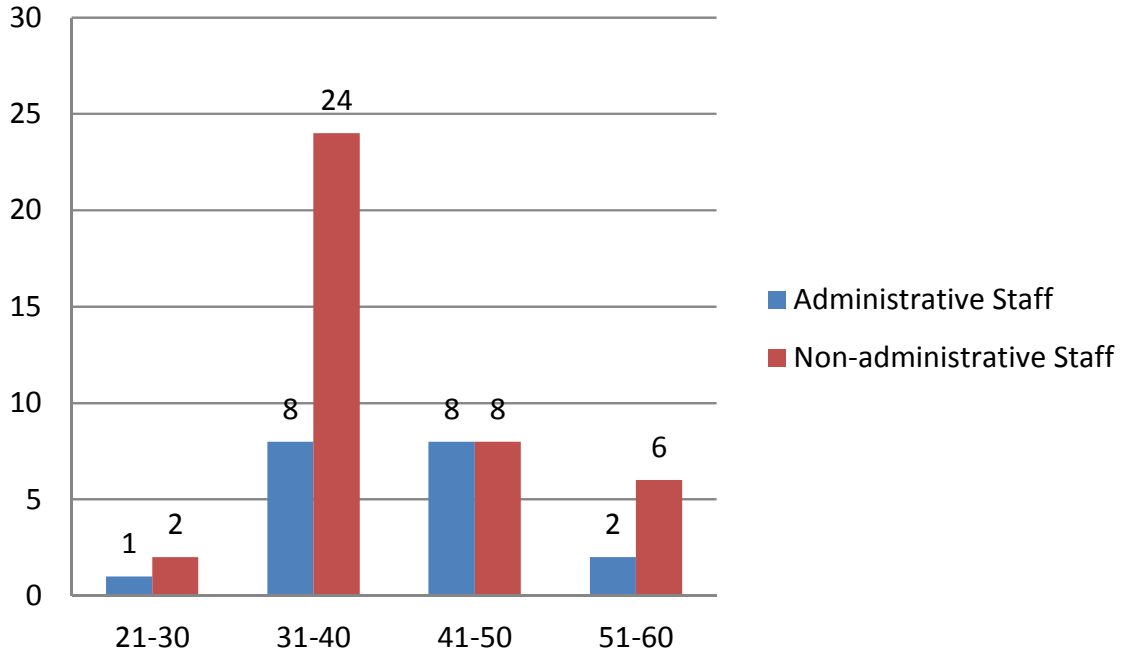


The data are shown as a percentage of all administrative and of all non-administrative employees, respectively, so as to normalise the data and compensate for the fact that there are more non-administrative than administrative staff. This facilitates cross-comparison.

With that in mind, it is obvious that the critical 41-50 age group is quite substantially under-represented among ENISA non-administrative staff. This age group represents just 20% of all non-administrative staff, versus 42% of administrative staff. This is precisely the age group where children are likely to need secondary education, and spouses are at the peak of their careers and too young to retire.

Figure 10 is similar to Figure 9, but shows the actual number of employees instead of the percentage of all administrative / non-administrative employees. We conjecture that the number of 41-50 year old non-administrative staff (8) would be roughly comparable to the number of 31-40 year old non-administrative staff (24) if ENISA's location played little or no role in recruiting and retention and if there were budget to hire them. This is the case for administrative staff (8 and 8).

Figure 10: Age distribution of administrative and non-administrative staff



A crucial concern is that ENISA's current management structure, with little permanent structure below the senior managers, would probably be unsustainable if the agency's size were to increase by a factor of two (as proposed by the Commission) or more. A related concern is that it may not be possible to simultaneously increase the staff size and maintain staff quality under the constraints imposed by the location.

Retention is not an immediate issue, but this should provide cold comfort. It probably means that those professionals who would have left are no longer accepting positions in the first place. A retention problem has thus effectively been transformed into a recruiting problem.

Once again, ENISA is not unique among decentralised European agencies. The previously cited Ramboll et al. study observes of decentralised European agencies in general: "The attractiveness of the agency's location for newly recruited staff is approximated by accessibility, presence of an international school, and exemption of national income tax." They found ENISA to be among seven decentralised agencies to have an "attractiveness problem", but did not rate ENISA's problem as "serious".

3.3.3.9. Generally weak links to European industry and to the European standards process

The finding of the 2007 evaluation was sound, and is confirmed by a survey conducted for ENISA in 2008 by GNKS that found that "…stakeholders assign ENISA deliverables high marks in terms of content and approach but view that efforts should be increased to foster their practical uses beyond the government and research community. … [G]overnment officials and national regulators have been the main clients of ENISA deliverables. The research and academic community has also proven to be users of the activities. Industry, however, has not featured well in this domain with the exception of its uses of deliverables dealing with the legal/regulatory implications and requirements for information and network security and risk management."

Our perception is that links to European industry are better than they were, partly because ENISA staff are far more visible than they were, but our interviews continue to raise concerns in regard to the ENISA's level of engagement with industry. This continues to be an area where concern is warranted; however, it appears to be primarily a matter of lack of staffing. Among competing priorities, this one may have also received less attention than one would like, but not necessarily less attention than it should have under the circumstances. There might be ways for ENISA to more effectively reach out to industry stakeholders – not only to producers of NIS products, but also to network operators, Internet Service Providers (ISPs), network equipment manufacturers, providers of web content and other Internet services, software vendors, and so on – but we have not identified specific programmatic weaknesses.

As regards standards bodies, ENISA put cooperative arrangements in place with the European Telecommunications Standards Institute (ETSI) in 2006, and is in the process of establishing arrangements with CEN/CENELEC.[110] Interviewees indicate that the arrangements with ETSI are working quite well. The arrangements with CEN/CENELEC may prove to be limited, since CEN/CENELEC's role in ICT security is limited, but could include important areas such as RFID and electronic signatures. We have found no indications that ENISA is unable to engage effectively with standards bodies where priorities and resources permit.

Thus, relatively weak links to industry and to the standards process apparently continue to represent a relative weakness, but the means of remediation seem to be fairly clear.

3.3.3.10. Low visibility overall

Lack of visibility was clearly a problem at the time of the 2007 evaluation, as is confirmed by the survey conducted for ENISA by GNKS in January 2008: "The Awareness of ENISA's deliverables is not as high as might be desired, even amongst the identified targeted audiences. Half of the respondents answering the Awareness question of a deliverable had never heard of it, and another 21% had heard of it but not read any of it."

Most stakeholders are of the view that ENISA is significantly more visible than it was years ago, partly because ENISA experts speak at a large number of well attended and relevant events. We would also note that these events are well distributed among the Member States, including smaller Member States and those that joined the EU in or after 2004. Dr. Helmbrecht's prestige has also been a positive factor.

Our view is nonetheless that ENISA still enjoys less visibility than it should, especially with relevant market players, and that this lack of visibility continues to be an issue.

[110] CEN is the European Committee for Standardization, or Comité Européen de Normalisation. CENELEC is the Comité Européen de Normalisation Électrotechnique.

4. POSSIBLE WAYS FORWARD

KEY FINDINGS

- Whether there is a formal change in ENISA's mission or not, its mission has grown and will continue to grow. The breach notification responsibilities of Article 13a of the Framework Directive and the need to conduct exercises (at European level and with third countries including the US) are examples of new high value-add activities that are effectively already part of ENISA's mission.
- ENISA is well led and well managed in our judgment, and the preliminary judgment of the Court of Auditors is that ENISA's finances are in order.[111] They are doing well enough with the resources that they have, but there are visible gaps – for example, in terms of their ability to engage with industry. These gaps are likely worsen as their mission inevitably expands.
- As far back as 2007, there were strong indications that ENISA's operational staff size was already insufficient to meet the full range of stakeholder expectations (see Sections 3.3.1 and 3.3.3.4). The mission has expanded at a far faster pace than the staff size, and is likely to continue to do so. An increase in headcount would appear to be in order.
- Simply increasing staff size is not the appropriate answer – it is also necessary to drive efficiency gains. Small improvements are possible in a number of areas.
- The largest single potential efficiency improvement would seek to address the travel inefficiency (and also the challenges posed to recruiting and retention) posed by ENISA's relatively remote location in Heraklion. The opening of a liaison office in Brussels, together with a branch office of modest size in Athens, would appear to represent a simple and cost-effective way to increase the number of missions that can be undertaken on average per staff year.

4.1. The Commission's proposed Revisions to the ENISA Regulation

The Commission's proposed new Regulation seeks to achieve a number of goals:

- ENISA's list of tasks are updated and reformulated broadly. The Commission seeks to achieve a balance so as to provide flexibility, while still being sufficiently precise to avoid confusion or ambiguity.
- ENISA's expertise is explicitly made available to the Parliament and the Council.
- Law enforcement and privacy protection authorities take part in the Permanent Stakeholders Group.
- Formalisation of the Management Board's authority to participate in strategic staff planning.

[111] Presentation of Eoin O'Shea at the European Parliamentary mini-hearing of 26 May 2011.

- Streamlining of procedures to correct well known defects in the current Regulation. For example, (a) simplified procedure for Management Board internal rules, (b) the opinion on the ENISA Work programme is provided by Commission services rather than via a Commission Decision; (c) the Management Board is also given adequate resources in case it needs to take executive decisions and implement them (e.g., if a staff member lodges a complaint against the Executive Director or the Board itself);[112] and (d) making it possible to extend the term of office of the Executive Director.
- A gradual increase of resources from the current authorised level of 57 to roughly 99 between 2012 and 2016 is anticipated.

4.2. Our view of the needs going forward

This section considers in general terms what should be done in our view in a range of areas.

4.2.1. Extension of ENISA's charter

As a first question, we consider whether ENISA's mandate should be renewed for a limited period of time, or indefinitely.

ENISA was initially established from 14 March 2004 for a period of five years.[113] The period was subsequently extended to eight years from the same 2004 starting date.[114] The Regulation was amended again to extend ENISA's lifetime *à l'identique*, this time by eighteen months, thus extending the duration of the ENISA until 13 September 2013.[115] The Commission's proposed replacement Regulation would provide for a period of five years from the new date of establishment.[116] ENISA has never had a permanent mandate.

When ENISA was first established, this time-limited charter surely made sense. There was no clear consensus that the function performed by ENISA was required, nor was there a consensus that an independent decentralised agency was the appropriate way to meet those needs.

Our assessment is that the agency pays a price for this uncertainty. It complicates recruiting and retention. It also limits the effectiveness of long term planning as regards ENISA's Work Programme.[117]

---

[112] Interviews support the view that these changes address genuine problems that have been visible over ENISA's history (see Section 3.3.3.3).

[113] Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency, Article 27.

[114] Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[115] REGULATION (EU) No 580/2011 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency as regards its duration.

[116] Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), COM (2010)521, Article 33.

[117] Uncertainties about the ENISA's longevity have interplayed with uncertainties about its location. When the Commission proposed in November 2007 to merge ENISA with a newly created European Electronic Communications Market Authority (EECMA), presumably in a different location, ENISA reportedly experienced higher than usual staff attrition for the year. See also the minutes of Management Board meeting 12 (March 2008), at http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1/mb_minutes_12.pdf.

At this point, we believe there is a widespread consensus that ENISA meets real needs.[118] We think that there is also a widespread consensus that an independent, decentralised agency is the most appropriate way to address these needs.[119]

We feel that the time-limited mandate for ENISA has outlived its usefulness. Today, the gain in flexibility is outweighed by the negatives.

One legitimate objection that could be raised flows from the Ramboll (2009) study,[120] which noted "… that established agencies are almost never reconsidered, except some agencies which have been established for a limited duration. Also, periodic agency evaluations do not in practice provide the opportunity to reconsider the agencies since the evaluations are not managed in a way that could result in reform or closure of an agency."

On balance, however, we feel that the time has come to provide ENISA with a substantially longer mandate. One option would be to provide a mandate that is not time-limited.[121]

Failing this, the new Regulation should, at a minimum, align ENISA's period of establishment with that of the next Multiannual Financial Framework (MFF), nominally 2014-2020. This seven year lifetime would somewhat increase the horizon for strategic planning for ENISA, would slightly benefit staff recruitment, and would have the advantage of aligning the ENISA planning cycle with that of other European institutions.

Recommendation 5. Provide ENISA with a longer period of establishment.

A new regulation for ENISA should either (1) not limit the time period for which it is established, or (2) align its period of establishment with the next Multiannual Financial Framework (MFF) cycle (2014-2020).

4.2.2. Expression of ENISA's mission in the Regulation

The 2007 Evaluation Report by a panel of experts and IDC found that different Member States had divergent views of the proper role of ENISA, and that these differences complicated the work of the MB (see Section 3.3.3.2).[122] Further, the MB had felt that there was tension among the various provisions of the 2004 ENISA Regulation that should be corrected in a future version (see Section 3.3.3.1).

[118] As the Commission noted in its impact assessment, the results of two previous consultations, the 2007 public consultation on the future of ENISA, and the 2008/2009 public consultation on possible objectives of a strengthened NIS policy at EU level and on the means to achieve those objectives, were consistent on this point, as was the 2007 evaluation. Our interviews and discussions are also consistent with the presence of a consensus on the need for ENISA.

[119] We think that the analysis of "Preferred Structure" that appears in Section 4.1 of the Commission's impact assessment (op. cit.) is substantially correct.

[120] Op. cit.

[121] This recommendation is not inconsistent with the Commission's impact assessment, which states: "Article 27 of Regulation 460/2004 indicated that ENISA would be established for a period of five years. Regulation 1007/2008 further extended this period to a total of eight years. When comparing with other Agencies, it can be concluded that it is rather exceptional to have a situation in which an Agency has a mandate that is limited in time. The limited duration of the mandate of ENISA is generally considered to be an important constraint for developing a long term vision and for attracting the relevant and qualified profiles for performing the highly specialized long-term nature tasks and a major reason for personnel turnover. Therefore, prolonging the mandate for an indefinite period, with regular review mechanisms, needs to be considered." At the same time, we are well aware that this recommendation may be controversial within the Council (see paragraph 7 of ST10296/11, 19 May 2011).

[122] The 2007 evaluation spoke of large Member States with established NIS capabilities having significantly different interests than smaller and/or newer Member States, which seems to still be the case. One interviewee suggested a possible linkage to the degree to which a Member State had its own domestic NIS industry.

Our interviews suggest that the concern about divergent interests is still relevant, although perhaps less intense than in prior years. Divergent interests are not necessarily a problem, in our view, as long as they do not impact the ability of the MB to function – part of the MB's job, after all, is to moderate among possibly different interests among the Member States.

If it is important to understand where the problems are in regards to ENISA's defined mission under the current Regulation, it is equally important to understand where they are not. The Commission has argued that the mission statement of ENISA suffers from *rigidity*.[123]

We do not find evidence of substantial rigidity in the tasks or objectives in the Regulation.[124] Through the Work Programme, the MB (in conjunction with ENISA staff and the PSG) has substantial ability to undertake new or different initiatives that are not inconsistent with ENISA's mission as long as they fit within the budget. That ENISA's mission has progressively expanded over the years would seem to argue that the description of ENISA's mission in the Regulation has not gotten in the way of its healthy evolution.

The concerns about *ambiguity* as regards ENISA's charter are, however, a real and continuing concern.

The distinction between ambiguity and rigidity is important relative to the path going forward. Reducing ambiguity and reducing rigidity have nearly opposite implications relative to how the Regulation should be revised. The former implies greater specificity in task definition, the latter implies less specificity. This also implies that, in reducing ambiguity, it is important to guard against eliminating needed flexibility.

As previously noted, the MB argued in their response to the 2007 evaluation for combining Article 2 (objectives) and Article 3 (tasks). In the abstract, we feel that objectives should not be mixed with tasks; however, we feel, as noted in Section 3.3.3.1, that the concern was probably inspired by the fact that many of the objectives in the 2004 Regulation were in reality scarcely distinguishable from being tasks.[125]

Recommendation 6. A revised Regulation should reduce ambiguity, but not at the expense of being overly rigid.

The scope, tasks and objectives in the Regulation should be revised so as to reduce ambiguities and reduce the risk of misinterpretation; however, reduction in ambiguity should not be achieved at the expense of needlessly increasing the rigidity of the revised Regulation in comparison with that of the current Regulation.

[123] "[I]t should not be overlooked that the key problems identified during the 2006/2007 evaluation of ENISA were *due to the rigidity of the original mandate* of ENISA (emphasis added) that was conceived in a different policy context (before the 2004 enlargement) and it has shown not to correspond to present and evolving NIS needs and challenges. Indeed, the list of tasks defined in Art. 3 of the current ENISA Regulation has been considered to be insufficient to provide the Agency with the necessary flexibility and adaptability to respond to the challenges of the continuously evolving NIS environment." Impact Assessment, op. cit. Section 2.2.

[124] We should add that, so far as we can see, the 2007 evaluation report considered the Regulation to be *ambiguous* but not *inflexible*, and our interview with an author of the study confirms this. The report refers to inflexibility of ENISA's *management*, not to inflexibility of its *charter*. It is the MB's response to the 2007 evaluation (not the evaluation itself) that complains of inflexibility, largely as a reflection of "…the concern that many Member States felt at the time that ENISA should not become an operational centre for European Networks" (see http://www.enisa.europa.eu/about-enisa/structure-organization/management-board/minutes-decisions-1/decision_09.pdf).

[125] This is equally true of the Commission's proposed Regulation in COM(2010) 521 final of 30 September 2010.

In revising the specification of the scope of ENISA, it is also necessary to consider a number of areas that were intentionally excluded from the 2004 Regulation, notably cybercrime and privacy. Under the post-Lisbon TFEU, it would be possible for ENISA to play a somewhat greater role in these areas. We consider these aspects in Section 4.2.8.

4.2.3. Operational or non-operational?

The degree to which ENISA should undertake operational functions has been a perennial point of contention, not only at the time that agency was created, but also periodically within the ENISA MB, and once again in the current process of determining whether and how to renew ENISA's mandate.

In its impact assessment, the Commission rightly observes: "ENISA was established as a platform for discussion among stakeholders. Therefore, it should be stressed that the Agency has no operational functions and is not equipped to carry out operational tasks of technical nature to enhance NIS."

This was clearly the case in the past. Should it also be so in the future? For that matter, is it even entirely true in the present?

Undertaking an operational role would have quite substantial implications for ENISA, not only in terms of the level of budget and staffing needed, but at many organisational levels as well.

In analysing the advisability of such a role, it is helpful to distinguish among different kinds of operational roles, since they do not all have the same implications. Key questions include:

- **Criterion 1:** Does the operation require handling data that is personally identifiable, or that otherwise potentially raises privacy concerns?
- **Criterion 2:** Does the operation require handling data that may be sensitive in terms of national or infrastructure or commercial security?
- **Criterion 3:** Does the operation require mission critical support in real time? Is it, in its nature, a 24 x 7 (all hours of the day or night, weekends and holidays included) operation?
- **Criterion 4:** To what extent does the operation overlap with existing activities (NIS, cybercrime, electronic privacy) within the Member State?

These questions imply substantial differences in the cost, the practicality, and the desirability of an ENISA role.

In working through the implications, it is worth noting that one moderately operational role *has already been assigned to ENISA* – the handling of security breach reports pursuant to Article 13a and 13b of the revised Framework Directive. Breach notification processing surely implies handling data that contains personally identifiable information, and that thus could raise privacy concerns. It also might entail sensitive information in regard to commercial security. It does not necessarily imply a 24 x 7 operation, and it does not necessarily create a substantial overlap with the activities of the Member State.

Handling information that is personally identifiable, or whose exposure might represent a violation of privacy, has implications for ENISA's personnel practices (staff must be trustworthy), for training, and for the security of data storage and data communication.

Handling information whose exposure could compromise commercial, infrastructure and/or national security has numerous implications. It is worth noting that ENISA does not currently handle highly sensitive information. Consider, for example, that no security

clearance arrangements are in place for ENISA. Handling sensitive data could, depending on the degree of sensitivity, have implications for ENISA's personnel practices (possibly including the need for security clearance arrangements for some staff members), for training, and for the security of data storage and data communication.

The need to operate in real time, around the clock, has significant implications. The most obvious is that one needs to have a crew available at all times, typically implying the need to operate over three shifts. Staff must not only be competent and trustworthy, but also willing to work inconvenient hours. This requires more staff than one might think, because one needs to have adequate coverage despite illness and vacation time. If the real time function is operationally critical, as will tend to be the case, it also implies the need for an *escalation path* – typically, the person who first answers the telephone will not necessarily have delegated authority to answer all possible questions, especially those that have significant implications for the safety of property or of human life. The escalation path typically runs to quite a high level – in the event of a major NIS incident, there might be an urgent need for the Executive Director or the chair of the Management Board to speak with stakeholders and the press.

For ENISA to take on an operational 24 x 7 role might also introduce the need for the first time for the MB to be able to respond quickly to some crisis. This need does not exist today, so far as we can determine. Neither the size of the MB nor the rules of the MB seem to be consistent with convening it in a hurry, nor do we consider it practical to convene this MB by a telephone conference. Some form of delegation of authority to a smaller group would likely be required.

Finally, we note that an operational activity that significantly overlaps with an existing Member State activity raises far more serious questions. Given that Member State activities often have an order of magnitude more staff than ENISA, is it even feasible for ENISA to undertake the function? Is a clear division of tasks and responsibilities possible? Is there an efficiency gain or some compelling value added in having ENISA play a European role in the process? Perhaps most important, would the activity be in conflict with the principle of subsidiarity?

Graphically, these considerations can be summarised as in Table 3. As one moves from left to right, the columns imply increasingly demanding responsibilities.

Table 3: Implications of various operational roles

	Handling of data with privacy implications	Handling of data with security implications	24 x 7 mission critical operation	Mission critical operation that overlaps Member State activities
Criterion	**1**	**2**	**3**	**4**
Hiring practices	X	X	X	X
Training in privacy practices	X	Possibly	Possibly	Possibly
Enhanced NIS security	X	X	X	X
Security clearances		X	Probably	Probably
Three shift operation			X	X
Escalation path	Possibly	Possibly	X	X
Changes to the MB			X	X

This analysis suggests a fairly clear-cut set of principles as to the degree to which an operational role for ENISA could be appropriate:

- Any operational role whatsoever for ENISA should be weighed carefully in terms of its costs and benefits.
- Operational requirements that meet only Criteria 1 and/or 2 (the need to handle data with privacy or security requirements) could be acceptable. The costs are not daunting, and ENISA will probably have too many of them in any case in conjunction with the breach notification responsibilities that it has already been assigned.
- Operational requirements that meet Criterion 3 raise a much higher threshold. They imply incurring costs that ENISA does not currently bear, and they imply numerous organisational adaptations. Nonetheless, operational requirements that meet Criterion 3 could be acceptable if benefits exceed costs.
- Operational requirements that meet Criterion 4 are probably unacceptable in general. They imply high costs, they risk duplicating functions that already exist in the Member States, and they raise subsidiarity concerns.

In our impact assessment in Chapter 5, we have not included any Options that correspond to Criterion 4 (24 x 7 activities with a substantial overlap with some Member State activity). In an impact assessment, options are supposed to have some realistic prospects for implementation; in our view, this would not be true for an Option that substantially duplicates existing operational programmes in the Member States.

4.2.4. Staff size, staff mix, and budget

The agency currently has an effective staff size of 57. The Commission, in its impact assessment estimates for its preferred option, Option 3, provides a budget as indicated in Table 4. We consider the proposed budget to appropriately reflect the assumptions that the Commission has made. This provides a useful starting point for the discussion.[126]

[126] Note, however, that the expected fraction of staff allocated to administrative work in 2015 and even more so in 2016 is implausibly low. If ENISA performs at the level of its peer group, one would expect 33 administrative staff in 2016, not 23 (unless overall staff productivity per employee were to improve by 43%, which seems unlikely).

Table 4: Commission's budget estimate for Option 3

Overview of budget under OPTION 3										
	Budget 2012	**%**	**Budget 2013**	**%**	**Budget 2014**	**%**	**Budget 2015**	**%**	**Budget 2016**	**%**
Administrative staff	21		21		23		23		23	
Operational staff	40		40		49		60		76	
TOTAL	**61**		**61**		**72**		**83**		**99**	
Breakdown of total budget										
EU Budget	9.262.000		9.449.000		12.109.087		14.918.281		18.824.525	
Third country contributions (EFTA)	222.288	100	226.776	100	291.818	100	358.759	100	351.788	100
Breakdown of total expenditure										
Title 1 – Staff expenditure (including recruitment expenditure)	6.031.824	64	6.239.860	64	7.866.298	62	9.528.461	62	12.073.953	63
Title 2 – Costs associated to the functioning of the Agency	559.017	6	570.256	6	647.328	5	727.256	5	841.176	4
Title 3 – Costs related to operational activities	2.893.447	31	2.865.660	30	4.193.179	33	5.051.323	33	6.361.183	33
Total expenditure	**9.484.288**	**100**	**9.675.776**	**100**	**12.706.906**	**100**	**15.307.040**	**100**	**19.276.313**	**100**

As the Commission notes, a staff of about 100 seems to be the minimum efficient size for a European decentralised agency. This is consistent with the recommendations of the 2007 ENISA evaluation report by an expert panel and IDC, and also consistent with the study of decentralised European agencies conducted by Ramboll et al.[127]

An obvious concern is that the 2007 evaluation had identified a staff size of "… about 100 staff, with the administrative and support personnel representing about 25-30% of the total …" as "…the appropriate size after 2009 …" The issue is that 2009 has come and gone. Many stakeholders were recommending similar staff size increases, or more, in the consultations in 2007 and 2009. In the Commission's preferred Option 3 budget, that staff size is not achieved until 2016.

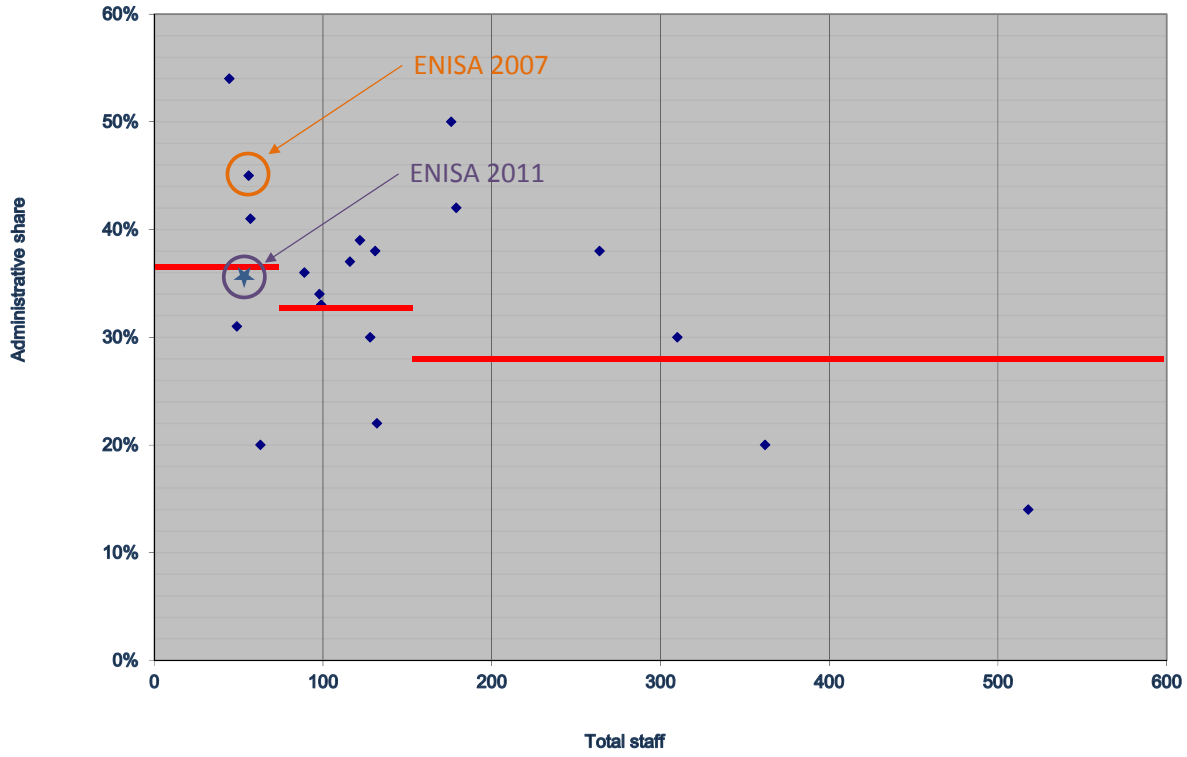
[127] Both are op. Cit.

Considering practical limitations, it may not be possible to do much better. There are challenges in hiring cybersecurity experts to work in Heraklion (see Section 3.3.3.8.2), and there are limits to the speed with which ENISA can absorb new staff.

A more immediate concern relates to the fact that the growth in workload comes sooner than the growth in staff size. The mission has already grown since 2007, it will continue to grow in 2012-2013, but the first substantial increase in staff does not appear until 2014. In its proposal, the Commission argues that it is impractical to increase headcount prior to 2014.[128]

Whenever implemented, an increase in staff size is likely to immediately generate modest improvements in the ratio of administrative staff to professional staff, which has long been a problem (see Section 3.3.3.5). Figure 11 depicts the relationship between agency staff size and the fraction of personnel fulfilling administrative functions.

Figure 11: The relationship between the size of a decentralised agency and the fraction of staff allocated to administration



Source: WIK-Consult GmbH, based on data from Ramboll et al. (2009) (based in turn on data from European Court of Auditors)

The red lines correspond to the averages for agencies of 0-75, 75-150, and more than 150 employees (namely 37%, 33% and 28%, respectively), as reported in the Ramboll (2009) study and based on data from the European Court of Auditors (please refer back to Table 2). They demonstrate the expected inverse relationship between the size of an agency and fraction of staff that is allocated to administrative functions. Given the relatively high administrative overhead of functioning as a European decentralised agency, large agencies are significantly more efficient than small ones.

[128] Impact assessment, section 6.1: "As regards 2012 and 2013, the budget estimations for the different options are aligned with the amounts set in the financial framework. This poses certain constraints, since the maximum allowed margin for deviation from the financial framework is 10%. Therefore, the actual implementation and impact of those policy options which foresee extension of the tasks of the Agency, and respectively of its resources, would start only in 2014."

A first observation is that, by this measure, ENISA is doing much better than it was in 2007. At that time, 45% of a staff of 56 was classified as administrative; today, 35% of a staff of 57 is classified as administrative, putting ENISA on a par with its peer group. As noted later in this section, we believe that this change reflects genuine efficiency improvements.

Increasing staff size does indeed serve to improve the ratio of administrative staff relative to total staff. At an agency size of less than 75, it is typical for 37% of staff to be classified as administrative; at a staff size between 75 and 150, the corresponding figure is 33%. Phrased differently, this means that an ENISA of 100 employees needs about 33 administrative staff, compared with the 37 that would be required if the agency functioned at the same level of efficiency that it does today.[129]

Note, incidentally, that this raises the concern that the Commission's budget projection for their Option 3 may be too optimistic as regards required administrative headcount. If ENISA performs at the level of its peer group in terms of agency size, an ENISA with 100 budgeted staff should require about 33 administrative staff for 2016, not 23. ENISA has made good progress in improving the balance between administrative and non-administrative staff, and can probably do still better, but expecting a reduction in administrative headcount from 37% to 20% of total headcount may be asking too much.

One additional observation flows from Figure 11. The dispersion in the ratio of administrative staff to total staff for small decentralised agencies is simply enormous. This would appear to suggest that there might be opportunities for less experienced or less efficient agencies to learn from those that are more experienced or more efficient. ENISA, to its credit, has been in contact with a few decentralised agencies where they have contacts, but this seems to us to suggest a missed opportunity at European level. The decentralised agencies would appear to face common challenges in dealing with substantial bureaucratic overhead. For each individual agency to pursue exchange of best practice through the contacts that they happen to have implies relatively high economic transaction costs and duplication, and also runs the risk that they will be seeking to import best practice from agencies that have their own efficiency problems. It seems that there might well be an opportunity at European level to provide a little coordination in order to systematically exchange best practice among the European agencies so as to improve the average efficiency of all.

Recommendation 7. Explore ways to exchange best practice as regard administration.

Explore ways to systematically exchange best practice among the decentralised European agencies in regard to efficient implementation of administrative procedures.

In our judgment, the problems with rigid staff structure (see Section 3.3.3.6) and with a high ratio of administrative staff to total staff (see Sections 3.3.3.5 and 4.2.4) have been dealt with and continue to be dealt with adequately at ENISA by the MB and the ED. We do not think that it is necessary to address them with sub-options in the impact assessment.

[129] Obviously, this must be a gradual function, not a step function at the point where the staff size increases beyond 75. It is trivial to generate a regression equation; unfortunately, the data is too "noisy" (i.e. the ratios for small agencies are spread too widely) for the regression equation to be statistically reliable.

4.2.5. Location and staff efficiency

The location of ENISA at the southern edge of Europe, with limited access to other Member States, contributes to higher travel costs, waste staff hours, and most important to lower staff efficiency (i.e. fewer missions per staff person-year). Section 3.3.3.8.1 quantifies some of these costs.

As we noted in Section 1.3, ENISA's location is explicitly not part of our terms of reference; however, staff size, budget, and efficiency are all essential elements of our terms of reference, and consequently ENISA's location is relevant to the extent that it impacts any or all of these.

There are a number of efficiency enhancements that must be considered within these constraints:

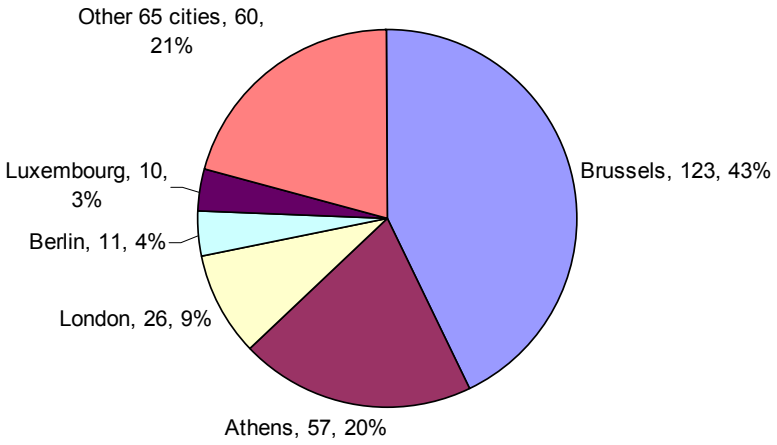
- Creation of a liaison office in or near Brussels (Section 4.2.5.1);
- Enabling some of ENISA's heaviest travellers either to work from a more easily reached location (presumably Athens), or else to spend a significant portion of their time telecommuting from a location with better air connections than Heraklion (Section 4.2.5.2); or
- As a thought exercise, considering the likely effects under the more extreme option of relocating all staff to an Athens office (Section 4.2.5.3).

4.2.5.1. Liaison office

The creation of a liaison office is not a new idea. It was specifically proposed in the 2007 evaluation; many of the responses to the 2007 consultation advocated a liaison office; and the idea has appeared in many of the reports that have subsequently appeared.

In principle, there could be benefit in a liaison office anywhere within a short train ride (say, two hours) of Brussels; however, review of ENISA travel records for the most recent twelve months (see Figure 12) strongly suggests that Brussels is far better than any other location. Of 287 missions that 18 ENISA "heavy traveller" staff conducted in 2010, representing two thirds of all ENISA missions, 123 (43%) were to Brussels. Since heavy travellers account for two thirds of all trips, this suggests just over 180 trips per year (assuming that infrequent travellers are about as likely to travel to Brussels as frequent travellers).

Figure 12: Destinations of ENISA missions by "heavy traveller" staff for the most recent twelve months



Source: WIK-Consult GmbH, based on ENISA staff estimates for June 2010 – May 2011.[130]

[130] ENISA, "Note for the attention of Mr Giles Chichester, MEP, Rapporteur on ENISA, ITRE Committee", 6 June 2011.

A liaison office in Brussels would not eliminate 100% of all travel to Brussels. First, there are some trips that as a practical matter require the personal participation of the Executive Director (or of another specific ENISA staff member by virtue of his or her unique role or knowledge). We believe, however, that a few well-rounded, senior experts based in Brussels could undertake a great many of the necessary liaison functions in Brussels on behalf of their colleagues based in Greece.[131] Second, there would be at least occasional need for the professional staff in Brussels to visit Heraklion in order to maintain contact and to stay abreast of developments there – otherwise, the risk is that they become less effective in representing ENISA in Brussels. Still, taking both of those factors into account, we estimate a net reduction of between 30 – 70% of current travel to Brussels. For estimation purposes, we assume a reduction of 50%.

What we envision is a small office with two or three senior professionals with wide background, together with an office manager. The professionals would whenever possible "stand in" for their colleagues based in Greece. This is a quite common model for European industry – many large corporations maintain a small office in Brussels in order to more effectively liaise with the European institutions.

Subject to availability of time, the Brussels staff might also undertake missions to nearby locations such as London (which is the third most frequently visited destination for ENISA).

The creation of a Brussels liaison office would create numerous benefits and economies, including:

- Avoidance of travel cost – instead of paying for flights and taxis, ENISA would bear only the cost of a fare on the Brussels public transport.
- Avoidance of waste staff time in travel – instead of some six and one half hours each way (ENISA estimate)[132] for 0.50 * 180 trips, travel time would in most cases be reduced to 30 minutes.
- Avoidance of needless wear and tear on ENISA staff. A reduction of 0.50 * 180 trips corresponds to a reduction of at least 20% in ENISA's total number of trips per year.
- The savings in time and wear and tear would mean that ENISA staff at the Brussels office could conduct at least two or three times as many meetings per year per staff member as would be possible based in Heraklion. This means that ENISA's interests would be far better represented than is the case at present, and also that stakeholders in the European institutions could be far better informed than is the case at present.
- The ability of ENISA to respond to last minute, urgent requests from the European institutions would be greatly enhanced.
- ENISA's ability to maintain its networks of contacts would be substantially enhanced.
- ENISA would be able to attend numerous events opportunistically that would not even be considered if attending meant a trip from Heraklion.
- ENISA's staff would build greater knowledge of Brussels-based institutions, and closer relationships, than could be done remotely.

[131] This is not something that can easily be analysed using existing travel records. At present, the agency would tend to be motivated to spread the travel widely among its experts so as not to over-burden them; with a Brussels office, the incentives would be reversed.

[132] ENISA, "Note for the attention of Mr Giles Chichester, MEP, Rapporteur on ENISA, ITRE Committee", 6 June 2011.

There would be, to be sure, costs as well. First, there is the direct cost of office space. Second, there is the additional administrative burden of maintaining the office (although we have not assumed a ratio of administrative to non-administrative staff that is different from that of the rest of the agency). Third, there is the substantial complexity of having to maintain operations and coordinate staff at a remote location for the first time. On balance, however, we think that the benefits substantially outweigh the costs.

Indeed, given the long history of this idea, we have some difficulty in understanding why it has not already been done. It was proposed as early as 2007. There is ample precedent for a decentralised European agency to maintain a Brussels liaison office – examples include CEDEFOP, EEA, EU-OSHA, EUROFOUND, FRONTEX, and OHIM.[133] The ENISA Regulation does not preclude it. It need not depend on additional headcount or budget – given the small investment involved, existing resources could simply be re-focused within the current budget. Given that the Brussels liaison office is within the decision scope of the Managing Board and the Executive Director, it could have been implemented at any time. Indeed, highly relevant to this discussion is that it is a significant operational efficiency that need not wait for the next MFF to come into force in 2014.

Recommendation 8. ENISA should open a Brussels liaison office.

ENISA should open a small Brussels liaison office as soon as practically feasible.

4.2.5.2. Locations other than Heraklion

For similar reasons, ENISA could achieve significant savings by permitting some number of senior "heavy traveller" operational staff to spend some significant portion of their time either permanently stationed or else telecommuting from one or more remote locations.

Two models are possible: One would be to establish a permanent office at a more accessible location, presumably Athens for reasons that we will explain shortly, and assign staff there on a long term basis; the other would be to permit staff to telecommute.

We have some preference for the first option (a permanent office) and a location of Athens because it better comports with the Council's decision to locate ENISA in Greece in first place, and with the Seat Agreement between ENISA and the Greek government. Indeed, the Greek government has already confirmed by letter ENISA's right to maintain an office in Athens as long as the Seat of the Agency does not move from Heraklion.[134]

There is an additional argument for having staff members who have close ties to the MB and/or PSG based in Athens. Of ENISA's 287 "heavy traveller" trips over the past twelve months, 57 were to Athens, and we believe that many of these were associated with MB or PSG meetings. It would be tempting to think that these staff could be based in ENISA's Athens office, but there are limits to what could be done – the Athens office space is not easily reached by public transportation, and it consists primarily of meeting rooms.

Our understanding is that the presence of international schools is not an issue in Athens. Given the presence of a diplomatic community, options in Athens are sufficient.

[133] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, part 3, Table 5.

[134] "Verbal Note" of the Ministry of Foreign Affairs of the Hellenic Republic, D.P.F. 3404/AS 3858, dated 8 September 2009. There would, of course, be things that need to be discussed, but we think that an accommodation could be reached under the right circumstances. This is not a radical option.

This implies that an Athens branch office might well be associated with some facilities cost. The Greek government has generously been paying the rent for ENISA's offices in both Heraklion and Athens, but it cannot be assumed that they would also do so for a third location (even if it were in Athens).

As with the Brussels office, it also involves some management complexity in dealing with personnel at multiple sites.

The optimal number of staff is not clear, but for purposes of estimation we have assumed that eight of ENISA's heaviest travellers would be allowed or encouraged to relocate and/or telecommute, on the understanding that this number might grow if ENISA's overall staff grows. In terms of pure economic efficiency, one might think that there is no limit to the number of staff who would more efficiently be located in Athens than in Heraklion; however, there are numerous practical constraints. First, we note that the heavy travellers will also tend to be among ENISA's most senior and most capable experts and managers. Assuming that the less senior experts remain in Heraklion, it is necessary that there be a critical mass of senior experts in Heraklion to lead, manage and motivate them. Second, we assume that not all operational staff would choose to leave Heraklion. Third, stationing a large number of ENISA staff permanently at a location other than Heraklion, even if it were Athens, might raise concerns with the host country government. We propose a contingent of six to ten senior "heavy traveller" staff because we believe that it is large enough (out of eighteen heavy travellers) to make a substantial difference, but still small enough at ENISA's current staff size of 57 that these other issues could be manageable.

The advantages of these arrangements are generally somewhat similar to those of maintaining a Brussels office. Travel costs would be reduced somewhat; needless wear and tear on staff would be avoided; the number of missions per staff year would be increased. This would also provide ENISA management with valuable flexibility as regards hiring a limited number of senior staff. This is true whether the first option (permanent placement) or the second (telecommuting) were chosen.

A telecommuting solution could support more cities, and might enable ENISA to maintain a network of "antennae" in a small number of Member States. There are potential benefits to a telecommuting approach in multiple cities, but somewhat less per staff member than with either a Brussels or an Athens office because (1) there is no other single European city that is visited as many times per year, (2) there would once again be the need for telecommuting personnel to be in Heraklion frequently enough to maintain good contact, and (3) these telecommuting arrangements could potentially introduce considerably more management complexity than opening either a single satellite liaison office in Brussels or a single branch office in Athens. Also, it would be necessary to carefully verify the compatibility of such arrangements with the Staff Regulations.

It is worth noting that there are examples of a decentralised agency maintaining operations in locations other than the Seat location, such as EUROPOL's Member State liaison offices.[135]

Recommendation 9. Consider assigning staff to a branch office in Athens.

ENISA should seriously consider assigning personnel on a long term basis to a branch office in Athens, subject to reaching suitable understandings with the host country government.

[135] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, part 3.

The opening of an Athens branch office would require careful planning,[136] but in principle, subject to availability of budget and to reaching any necessary understandings with the Greek government, it need not wait for the next MFF beginning in 2014. Indeed, with suitable approvals, a small prototype office could be opened almost immediately using ENISA's existing Athens facilities.

We view an Athens branch office and/or telecommuting as complementary to a Brussels liaison office, not as mutually exclusive alternatives to a Brussels liaison office.

4.2.5.3. Relocating staff to Athens altogether

In order to understand the relative merits and efficiencies of the different options, it is helpful as a thought exercise to contrast them with the more extreme option of relocating *all* staff to an Athens office.

In terms of pure efficiency in the long term, it is clear that having ENISA staff located in one location in Athens would be superior either (1) to having all ENISA staff in Heraklion as is the case today, or (2) to having some ENISA staff based in Heraklion and some in Athens.

A move to Athens would, however, raise a number of complexities:

- It raises far more issues relative to formal and informal understandings with the host country government.
- Some staff would welcome a move to Athens, but not all. Presumably, there would be some attrition, especially but not exclusively among locally hired staff.
- It would be necessary to find a new location with a sufficient number of offices to accommodate current and mid-term future ENISA staff. The facility would have to located in proximity to public transport. The existing Athens facility is neither large enough nor suitably located.
- It cannot be assumed that the Greek government would pay the rent for such a facility.
- Any synergies with FORTH would be sacrificed.
- Finally, one must consider the disruption and cost that always accompany a large scale office move.

The advantages are straightforward. The inefficiencies noted in Section 3.3.3.8 would be directly and fully addressed. Athens has a full flight schedule, summer and winter, to a great many European destinations. International schools are reportedly not an issue. Jobs for spouses might still be an issue, but probably less of an issue than in Heraklion. Cultural facilities are more extensive. Recruiting and retention would tend to be easier.

As previously noted, ENISA currently hires three full time staff to handle travel arrangements due to the high complexity of travel to and from Heraklion. If the agency were located in Athens, the complexity of travel would be greatly reduced. This might make it possible to use centralised Commission travel services or otherwise reduce this high burden (which amounts to 5% of staff at present).

[136] In fact, two studies of how to use an Athens office were undertaken years ago, but whether they are relevant to the agency as it is today would need to be assessed.

We have looked at these issues, but they are far more complex than we could hope to resolve in such a short study. We would not reject the idea out of hand, but we think that the balance of benefits to costs is far less obvious than in the case of an Athens office. The case for a Brussels liaison office is compelling. The case for an Athens office seems to be strong. The case for moving all staff to Athens, leaving aside the question of whether it is appropriate to do so, is probably positive in the long term but is mixed in the near term.

4.2.6. Synergies with FORTH in Heraklion

ENISA is hosted on the campus of FORTH, a prominent research institute interlinked with the University of Crete. FORTH is active in NIS research, and itself operates a CERT.

There are numerous forms of cooperation and interaction between ENISA and FORTH. FORTH provides a certain portion of the IT infrastructure used by ENISA (including switchboard and high speed Internet access), but operational cooperation in regard to NIS for ENISA seems to be limited. FORTH also cooperates with ENISA to offer summer training to NIS professionals. ENISA employees are entitled to access to various FORTH and university facilities, including the cafeteria, library, and athletic facilities. FORTH and ENISA have sometimes cooperated on conferences relevant to NIS.

Nonetheless, interviews with ENISA and with FORTH suggest that the full range of synergies have probably not been fully considered or exploited. We therefore recommend that ENISA and FORTH nominate a small committee to study potential further synergies for, say, six months, and report back to both institutions. Any recommendations should, of course, pay attention as appropriate to European procurement regulations.

Recommendation 10. Explore possible further synergies with FORTH.

Senior management of FORTH and ENISA should task a small committee of their respective experts to explore whether there might be additional synergies between the two organisations. The committee's report should be made available to the ENISA MB.

4.2.7. Management Board (MB) size and structure

We have considered carefully the concerns raised about the MB being too large and too unwieldy. In general, we do not feel that this MB is structured in a way in which such an MB should be structured; however, there does not seem to be a compelling case for a massive re-structuring.

Many stakeholders have also argued that the current structure ensures that the MB can provide outreach into governments in every Member State. One argued that the MB has found joint meetings with the PSG useful, which is to say that an even larger constellation could be effective.

Relative to the MB's current tasks, we see no compelling need for a smaller MB, nor for the MB to establish a smaller "executive committee".

If the MB were to take on responsibilities that required a more immediate response, or if ENISA were to take on tasks with a more immediate, operational role, then it would probably be necessary to re-think the structure of the MB so as to enable meetings on short notice or by telephone conference.

4.2.8. Missing functions and gaps

In most areas of NIS, including both cybersecurity and CIIP, ENISA's role has progressively expanded within the scope of its existing mandate, subject primarily to the constraints of budget and staff resources and the prioritisation that this implies.

There are, however, a number of areas where ENISA has done less work than it might have, including cybercrime, privacy / data protection, and the military, all of which typically have institutions and communities of interest that are somewhat distinct from those of ENISA. ENISA has also been less engaged with businesses and consumers than it might have been, and has engaged on a sustained basis with only two standards bodies. Finally, ENISA has engaged on a regular and sustained basis with only a small number of potential international stakeholders.

4.2.8.1. Cybercrime

The 2004 ENISA Regulation includes restrictions on ENISA's ability to engage in a number of areas relating to public safety and law enforcement.[137] Nonetheless, ENISA is increasingly involved in these issues.

Irrespective of ENISA, specific regulations, action lines and collaboration forms for combating cybercrime are already in place. Important organizations include Europol and the European Cybercrime Task Force, an expert group made up of representatives from Europol, Eurojust and the European Commission that works together with the Heads of EU Cybercrime Units. There are also plans to establish a European Cybercrime Centre (action 31 of the Digital Agenda for Europe).

ENISA should liaise with these organizations, contribute its NIS expertise, and share NIS good practices and views with the cybercrime community.[138] ENISA can learn from this liaison with the cybercrime community which problem areas exist and what trends are developing.

Concretely, ENISA's 2011 Work Programme[139] includes a Work Package with two deliverables: (a) production of a "Good practice for CERTs in addressing NIS aspects of cybercrime" document, and (b) the sixth ENISA workshop for CERTs in Europe. Today, the CERTs and the cybercrime / law enforcement communities work in their own respective sub-domains of NIS, with little dialogue between them. The "Good Practice Guide" seeks to be a collection of best practice from mature European CERTs, including roles and responsibilities, workflows, and cooperation with other key players. The intent is to shed light on commonalities and differences between the work of the CERTs and the related work of law enforcement in order to better understand barriers to cooperation and how they might be addressed.

The liaison function should focus on information exchange on a generic level, but should probably not include the exchange of specific and detailed data in light of the special requirements for handling cybercrime related data.

---

[137] Article 1 of the 2004 Regulation states: "The objectives and the tasks of the Agency shall be without prejudice to the competencies of the Member States regarding network and information security which fall outside the scope of the EC Treaty, such as those covered by Titles V and VI of the Treaty on European Union, and in any case to activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law."

[138] For example, a Memorandum of Understanding with Interpol is under discussion.

[139] See ENISA, Work Programme 2011, Securing Europe's Information Society, 30 November 2010, Work Package 1.5: "CERTs role in supporting the fight against cybercrime".

4.2.8.2. Privacy and data protection

Much the same applies to privacy and data protection. ENISA can play an important role in assessing the data protection aspects of current and new on-line services, and providing independent advice on issues on the boundary between NIS and privacy. ENISA already plays a key role with respect to the related subject of data breach notifications.

The linkages between security and privacy were always present, and are perhaps becoming increasingly relevant. ENISA's 2011 Work Programme includes, for instance, a Work Package on "Security and privacy in the 'Internet of Things'",[140] which builds on previous ENISA Privacy Impact Assessment (PIA) work. Work Stream 3 includes a Work Package on "Deploying privacy & trust in operational environments". The 2010 Work Programme included a "Stock taking of authentication and privacy mechanisms" Work Package that addressed notion of identity in ICT applications and services, an issue squarely on the boundary between security and privacy.[141]

In 2010, ENISA worked together with the European Data Protection Supervisor (EDPS) on the assessment of the current situation concerning the introduction of a European data breach notification requirement for the electronic communication sector. Under the Work Package "Supporting the implementation of the e-Privacy Directive (2002/58/EC)" of Work Stream 3 of 2011 Work Programme,[142] ENISA is continuing to collaborate with the Article 29 Data Protection Working Party, the EDPS, and the European Commission (DGs JUST and INFSO) and has as its objective to investigate how to practically implement at EU level the new data protection provisions of Article 4 of the e-Privacy Directive.

4.2.8.3. The military

ENISA has had a number of contacts with both NATO and the European Defence Agency (EDA) over the last year. The goal of these contacts has been to explore opportunities for information sharing and, in the long-term, a more active collaboration. Current guidance to ENISA is to limit its contacts with NATO to exchange of information. A more active collaboration could be envisaged if there were a request from the European External Action Service.

There is, however, considerable potential to move further in the future. ENISA could play a useful role in facilitating increased dialogue between communities that are currently working largely in isolation. Increased collaboration between these communities is a logical consequence of the Lisbon Treaty, but it is clear that any dialogue would benefit from a structured approach. Bringing together communities to build a stronger NIS culture is completely aligned with the mission of ENISA.

ENISA is an observer in EDA's Ad Hoc Working Group on Cyber Defence, and is collaborating with EDA primarily by assisting the Agency in understanding the work that ENISA has done in various areas of interest (such as Cloud Computing and CIIP). This level of collaboration appears to benefit both parties. ENISA reportedly has found it useful to understand the kind of initiatives that are being pursued by these communities and possible synergies and gaps for the future.

---

[140] ENISA, Work Programme 2011, Securing Europe's Information Society, 30 November 2010.
[141] ENISA, Work Programme 2010, Build on Synergies – Achieve Impact, apparently undated.
[142] ENISA, Work Programme 2011, Securing Europe's Information Society, 30 November 2010.

An ENISA manager reports that the military tends to be "… working on the same problems as our own stakeholder community. In addition, the two communities often have extremely similar objectives and it is frequently only terminology that masks this fact (hence, military communities may hold conferences on Cyber warfare, but are extremely interested in protecting critical infrastructure and all communities are concerned with identifying and responding to cyberattacks). One of the ways in which ENISA was able to provide useful input to EDA, was to explain and interpret the work we have done in the area of Cloud Computing. Understanding the security issues associated with developing technology or business models is something that all communities will have to deal with in the future - this is therefore a good example of where efficient information sharing is a win-win situation for all the communities involved."

4.2.8.4. Businesses, consumers, academia, and standards bodies

Relative to businesses, consumers, and academia, ENISA's links are not as strong as they should be in our judgment.[143] This is primarily a result of conscious prioritisation in light of limited resources.

A number of relevant businesses are represented on the ENISA Permanent Stakeholders' Group (PSG). The PSG serves not only as a source of *input* to ENISA, but also as a vehicle for *outreach*.

ENISA has potential interactions with a huge number of external stakeholders.[144] Some of these are industry bodies or Public Private Partnerships (PPPs). ENISA maintains numerous relationships with these entities, but overall their interactions with private entities tend to be less intense than their interaction with governmental or quasi-governmental entities.

ENISA maintains visibility with businesses, primarily through an active calendar of speaking engagements. Otherwise, there does not appear to be any consistent, programmatic attempt to reach out to businesses or consumers. This is arguably a gap.

Interviewees felt that ENISA could be playing a greater role, for instance by hosting meetings among businesses to share incidents. There was a sense that ENISA reports are of high quality, but it is not clear that they are visible to businesses or much used. "ENISA should be more active in distributing their reports, and giving advice to the business." One interviewee noted that there are many different kinds of businesses, including technology suppliers and technology users. "ENISA may play a role to play here to synthesize conflicting needs."

Links to the standards bodies were identified as a weakness in the 2007 review, but shortly thereafter a relationship with ETSI was put in place that appears to be working well, and a relationship with CEN/CENELEC is under discussion (see Section 3.3.3.9). There is more that could be done if more resources were available, but we do not perceive a programmatic failure.

4.2.8.5. International

Relative to international relationships with the many bodies active internationally (see Section 2.6), ENISA is visible in many but active in only a few.

[143] This was identified as a weakness in the 2007 evaluation, and also by the Commission in its 2010 impact assessment report.

[144] See "Country Reports", prepared for ENISA by IDC, 2009.

ENISA is active in the EU-US Working Group on Cyber Security and Cybercrime. The activities in different areas are expected to be conducted primarily via Expert Sub-Groups (ESG). ENISA will play an active role in the ESGs that are devoted to Public Private Partnerships (PPP), Cyber Incident Management, and Awareness Raising.

There are occasional interactions with countries outside of Europe, as for instance when a Chinese ministerial delegation visited ENISA in 2010. There do not appear to be a great number of such interactions. Some interviewees suggested that ENISA's location in Heraklion may be one of several limiting factors.

As a result of its 2011 Work Programme, ENISA has frequent interaction with the International Telecommunication Union's (ITU) activity on the economics of information security.

In most international bodies, however, ENISA is visible only to the extent that it periodically makes high profile presentations.[145] There is no regular, programmatic interaction with the OECD, the G8, the Council of Europe, or the OSCE, for instance.

We thus have the sense that ENISA is not currently able to represent Europe as well as it ideally could in the multitude of fora outside of Europe; however, its extensive current engagement in EU-US exercises (a very good use of resources in our view, and a task that would be extremely difficult to orchestrate if ENISA did not exist) seems to demonstrate that it has the necessary capability.

Rather than a specific programmatic weakness, the main issue seems to be legitimate prioritisation decisions that have been taken in a context where ENISA does not have enough resources to take on everything that it ideally ought to take on. ENISA has determined to focus on (1) Europe, (2) the United States, (3) Asia, and (4) the rest of the world, in that order. We consider this entirely appropriate under the circumstances; at the same time, it appears to represent a missed opportunity for Europe.

4.2.8.6. Overall

We think that some clarification in a future revision of the ENISA Regulation is in order, but the current Regulation does not appear to have prevented ENISA from engaging with cybercrime or with privacy / data protection stakeholders. The relationship to the military would benefit from clarification.

Recommendation 11. Clarify ENISA's ability to engage with privacy / data protection issues and cybercrime issues, and clarify its relationship to the military.

Any revision of the ENISA Regulation should clarify ENISA's ability to engage with privacy and data protection stakeholders, to enable ENISA to support these activities, subject to due respect for the principle of subsidiarity.

We have not identified current problems with ENISA's linkages with the various communities with which it needs to engage other than those caused by limited resources and the prioritisation that necessarily attends it.

[145] See, for instance, "Helmbrecht at Council of Europe "Octopus" cyber crime conference", at: http://www.enisa.europa.eu/media/news-items/council-of-europe-and-enisa-on-cyber-security.

Overall, ENISA seems to be able to find ways to engage with its various stakeholder communities so as to support them with dialogue and exchange of best practice, but not to inappropriately get in their way. The key issue seems to be one of resources (see also Section 5.3.3).

Recommendation 12. Seriously consider increasing ENISA's budget.

Consider seriously increasing ENISA's budget and staffing so as to enable it to engage more extensively with industry and consumers, global counterparts, and standards bodies.

5. AN ABBREVIATED IMPACT ASSESSMENT

KEY FINDINGS

- This chapter provides an impact assessment with a different thrust than that of the Commission; however, there are many points of commonality with the Commission's impact assessment.
- As noted in Chapter 4, ENISA's effective mission has grown, and can be expected to continue to grow.
- In light of efficiency and effectiveness considerations, it makes sense to consider options that reflect a blended strategy of efficiency gains and headcount increases. Efficiency gains may be particularly crucial to deal with the period 2011-2013, since the mission will predictably grow before it is possible to substantially increase staff size.
- We include an impact assessment Option where a CERT for the European institutions is organised as part of ENISA. We see both pros and cons to doing so, and we recognise that this issue is currently under study by the pre-configuration team, but we think that it is important to raise this as a possible evolutionary path for ENISA.

This chapter of the report provides an abbreviated impact assessment, providing a number of options that represent different evolutionary paths for ENISA going forward. It differs in many respects from the impact assessment that the Commission has put forward.[146]

As noted in the Introduction, in principle there is always the question: should the agency continue as it is, should it be abolished, or should it be changed going forward? In this case, the answer at this level of discussion seems to be fairly clear: ENISA needs to be strengthened and streamlined in order (1) to more efficiently meet current challenges, and (2) to meet the expanding demands to which it is continually subject.

The European institutions (the Commission, Parliament and Council) routinely use an impact assessment as a standard instrument to answer such questions. The impact assessment serves to evaluate the merits of any of a wide range of possible policy initiatives, including the creation or renewal of a programme.

The Commission has put forward a proposed revision[147] to the Regulation that established ENISA,[148] and has as required accompanied that proposal with an impact assessment.[149]

---

[146] SEC(2010) 1126, Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA).
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1126:FIN:EN:PDF.

[147] 2010/0275 (COD); Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA), COM(2010)521.
http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0521:FIN:EN:PDF.

[148] Regulation 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency.

[149] SEC(2010) 1126, Commission Staff Working Document, Impact Assessment, Accompanying document to the Proposal for a Regulation of the European Parliament and of the Council concerning the European Network and Information Security Agency (ENISA).

As noted in Section 1.1 of this report, we felt that the Commission's impact assessment did not meet our needs for this report. First, the baseline for analysis seemed to us not to sufficiently distinguish between future activities and activities that are, for all practical purposes, part of ENISA's active mission today (and which are appropriately viewed as representing part of the baseline for analysis). Second, the options were drawn in such a way as not to offer real, meaningful choices. In our view, they did not address many of the real challenges facing the agency. In consequence, the analysis of impacts was not relevant.

Notably, we felt that the Commission's impact assessment paid insufficient attention to the numerous challenges to efficiency and effectiveness that ENISA already faces, many of which had been identified in the 2007 evaluation but were never addressed at European level (see Sections 3.3.1 and 3.3.3). ENISA's mission has already unavoidably grown since 2007,[150] creating additional challenges and amplifying some of those that had already been identified.

With this in mind, the absence of an option to address current limitations to ENISA's efficiency and effectiveness is conspicuous.

We felt it necessary to construct our own impact assessment in abbreviated, "skeleton" form. We emphasise that our terms of reference did not require us to create an impact assessment – we did so because we felt that there was no other way to properly carry out the assignment under the circumstances.

Under the Commission's 2009 Guidelines,[151] the impact assessment consists of:

- Procedural issues and results from consultation of interested parties.
- Policy context, problem definition, and subsidiarity.
- Objectives.
- Policy options.
- Analysis of impacts.
- Comparing the options.
- Monitoring and evaluation.

Many of these required elements are of limited interest to readers who are not specialists in impact assessment methodology; moreover, we had no major issues with large portions of the Commission's impact assessment. Those who wish to review the procedural issues, the analysis of subsidiarity, or the objectives are invited to read the Commission's impact assessment.

Instead, we have concentrated here on (1) development of options and sub-options that address current and future challenges, and (2) analysis of impacts of these revised options and objectives.

http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=SEC:2010:1126:FIN:EN:PDF.

[150] Consider, for example, ENISA's explicit role in regard to breach notification, as mandated in Article 13a of the revised Framework Directive that was enacted in 2009. These provisions are just now taking effect.

[151] Impact Assessment Guidelines, 15 January 2009, SEC(2009) 92.

5.1. The nature of the problem

The relevant problem here is not NIS in general; rather, it is the need for coordination, cooperation, and exchange of best practice at European level.

There is something of a consensus that ICT incident response at national level is *not* ENISA's role. Most Member States already have CERTs, and many of these organisations are an order of magnitude larger than ENISA. As a representative of the Finnish CERT noted at the Parliamentary mini-hearing on 26 May 2011, these CERTs welcome ENISA's support, coordination, exchange of best practice, and provision of training, and have appreciated ENISA's role in conducting exercises at European level, but would not welcome an operational role that interferes with their ability to carry out their mission at national level. Moreover, for ENISA to take on such a role might well be inconsistent with the principle of subsidiarity.

At the same time, a few potential operational responsibilities have been identified for ENISA, and in some instances ENISA is already tasked to perform in these roles. For example, Article 13a of the revised Framework Directive tasks ENISA with (1) receiving, where appropriate, individual incident reports of any "… breach of security or loss of integrity that has had a significant impact on the operation of networks or services"; (2) receiving annual reports; and (3) advising the Commission in regard to technical measures to achieve harmonisation. This is a fine example of the role that ENISA can play – in the absence of this kind of coordination, it would be impossible to develop meaningful statistics or overviews at European level. We emphasise that this is a *current* role, not a future or speculative role.

ENISA faces many challenges, most of which were already visible in the 2007 evaluation (see Sections 3.3.1 and 3.3.3). Some of these have been mitigated to some degree in the intervening years, but others remain. Particularly noteworthy are:

- Insufficient staff and budget, not only relative to future demands, but also to current demands;
- Inherent inefficiencies as a result of (1) the small size of the agency, and (2) travel necessitated by the agency's remote location.

The problem definition thus needs to consider not only (1) the ability to respond to the steady expansion in demands for ENISA's services, but also (2) the need to increase ENISA's efficiency and effectiveness in meeting the demands that it already has.

The problem that ENISA seeks to address at European level includes:[152]

- the fragmentation of national approaches to tackling the evolving challenges;
- the lack of collaborative models in the implementation of NIS policies;
- the insufficient level of preparedness also due to the limited European early warning and response capability;
- the lack of reliable European data and limited knowledge about evolving problems;
- the low level of awareness of NIS risks and challenges;
- the challenge of integrating NIS aspects in policies to fight cybercrime more effectively.

[152] This list is drawn from the Commission's impact assessment.

As regards subsidiarity, these challenges cannot be addressed at Member State level alone. They cannot be addressed by voluntary coordination among national agencies – the number of coordinating entities is too great, the transaction costs would be prohibitively high. Finally, as the Commission's impact assessment rightly notes, ICT systems in Europe are increasingly interlinked, and a chain is only as strong as its weakest link.

The need for action at EU level is manifest. Weaknesses in ICT systems in one Member State could create exposures for ICT systems in other Member States – the costs of a failure to act at European level could be substantial.

5.2. Policy options

This analysis is premised on the following set of options (which differ significantly from those in the Commission's impact assessment).

Table 5: List of options

Policy option	Description
OPTION 1: No policy	The ENISA mandate expires; however, other activities at European and Member State level continue without change.
OPTION 2: Business as usual	On 14 March 2012, the mandate of ENISA is further extended. Mission: • To the extent that ENISA's mission has already expanded, those changes carry forward. • To the extent that ENISA's mission would likely expand within the scope of the current Regulation, those changes are also reflected. Only small increases in staff are assumed. Only small increases in efficiency are assumed.
OPTION 3a: Same mission, enhanced resources	Same mission as in OPTION 2. Increase in staff size begins in 2012.
OPTION 3b: Same mission, enhanced resources and efficiency	Same mission as in OPTION 2. Increase in staff size begins in 2012, but more slowly than in OPTION 3a. Emphasis on increased staff efficiency, especially as regards travel and recruitment. A Brussels liaison office and a small branch office in Athens are assumed.
OPTION 4: Add a CERT for EU institutions to ENISA's mission.	Same mission as in OPTION 2, plus a CERT for the EU institutions. Staff needs to expand to enable an operational 7x24 role, and an expanded Brussels liaison office. This Option assumes the same efficiency gains as in Option 3b, and staff growth for functions other than the CERT that is also in line with Option 3b.

The "no policy" option, which would signify an end to ENISA, is required in every impact assessment.

Similarly, it is routine for an impact assessment to consider a business as usual option, which often serves (as it does here) as a baseline for comparison of all other options. In this case, the baseline needs to consider extensions to ENISA's mission that are already in place (for example, new breach notification responsibility) to be part of the baseline. The baseline is also assumed to include minor efficiency improvements to the functioning of the agency, and these are assumed to carry forward into options 3a, 3b, and 4.

Options 3a and 3b reflect two sets of sub-options. In the first, the mission is as in the baseline, and minor efficiency improvements from the baseline are included. Additional headcount and budget are provided, but no other changes are made.

Option 3b differs from Option 3a in that various measures are taken to ameliorate some of the efficiency constraints to which the agency is subject (and which were already identified in the 2007 evaluation), including a number that seek to ameliorate the effects of ENISA's location in Heraklion. Notably, a Brussels liaison office with three senior staff and a branch office in Athens with eight senior staff are assumed. These measures enable the agency to fulfil the same objectives with somewhat less headcount and budget.

Option 4 represents a more radical change. In the Digital Agenda for Europe adopted in May 2010, the Commission committed itself to establishing a CERT for the EU institutions, as noted in Section 2.4.2. The EU institutions have set up a CERT pre-configuration team made up of IT security experts from the EU institutions. It is clear that ENISA will play some role relative to this CERT. Option 4 contemplates housing the European CERT within ENISA.

5.3. Analysis of impacts

This section evaluates the likely impacts of the various Options.

5.3.1. OPTION 1: No ENISA

The guidelines for conducting an impact assessment require consideration of discontinuing the policy intervention in question altogether. Other relevant initiatives (for example, at Member State level) are assumed to remain in place.

We list the option here for formal completeness, but we will not dwell on it. We think that a clear consensus has emerged that the function that ENISA performs is needed at European level, and that an independent agency is the most appropriate vehicle with which to implement it.

5.3.2. OPTION 2: Business as usual

In an impact assessment exercise, it is important to establish a "business as usual" case so as to provide a baseline against which other options can be compared. Here, we assume a continuation until 2020, and a set of responsibilities that reflect what the agency either is already doing or is already committed to do.

We assume that certain efficiency improvements that are already reflected in the Commission's proposed Regulation are included in the baseline – for example, the annual Work Programme will not need to be approved by means of a Commission Decision.

In understanding the real baseline, it is important to consider not only the provisions of the ENISA regulation, but also the missions that the agency actually performs, or is already committed to performing. This is particularly true because ENISA's charter gives it substantial ability to undertake new tasks, subject to approval through the annual Work Programme, so long as they are achievable within its staffing and budget.

The baseline thus includes not only activities that ENISA has performed for years, such as assisting the CERTs, but also many activities that are consistent with ENISA's mandate under the 2004 Regulation, but that were only identified in recent years. These additional activities include:

- Conducting exercises at European level and with partners such as the US (see Section 2.6.5).
- Assisting with security breach notification data as envisioned in the Framework Directive as revised in 2009 (see Section 2.3.4).
- Participating in the expert group that is evaluating the creation of a CERT for the European institutions (see Section 2.6.5).
- Increased interaction with CIIP stakeholders and groups (see Section 2.3.3).
- Increased interaction with data protection and cybercrime stakeholders and groups in order to exchange best practice (see Sections 2.3.4 and 2.3.5). This is to some extent already the case, but we assume that existing restrictions in the 2004 Regulation would be eased or eliminated.
- Increased interaction with a range of international stakeholders and bodies (see Section 2.6).

As a guiding principle, in Option 2 (and also in 3a and 3b), ENISA undertakes no operational role that entails 24 x 7 operation (Criterion 3 in Section 4.2.3), nor any operational role that supplants a mission critical in a Member State (Criterion 4 in Section 4.2.3).

One should in principle also consider what activities could be dropped. The fact that ENISA is performing a function today is not, from the perspective of an impact assessment, dispositive. Our sense is, however, that the current Work Programme development process and the current management team do a reasonably job of managing priorities, and that the agency's current activities provide good return overall on the resources invested.

The effects of Option 2 are fairly straightforward to predict. ENISA already has a mandate somewhat larger than what it is staffed to do. It does well with many core constituencies, such as the CERTs, but has limited resources to address a wide array of needs. ENISA staff, the MB, the PSG and the Commission establish priorities through the Work Programme. Under these priorities, in light of the underlying shortage of resources, there is less time to spend with the commercial sector, consumers, the standards community, and various international partners than would be ideal. It is engaged with some stakeholders, but necessarily ignores others. Data collection was always a part of ENISA's charter, but ENISA has analogously never had the resources to seriously embark on data collection.

ENISA's mission has grown, and will continue to grow. For ENISA, the *need* for old missions has rarely disappeared. With constant staffing, new missions could only be undertaken by reducing commitments to existing missions.

The areas that are neglected today would likely continue to be neglected. Some activities that are served today might be served less well, or not at all. Some new missions would be neglected, not because they were lacking in merit, but because they were deemed less meritorious than other crucial missions that were being served with scarce budget or resources. The exact choices would be made through the Work Programme, and cannot be predicted today, but the effects of resource scarcity in the face of steadily growing demands are predictable in general.[153]

[153] These observations are generally consistent with those of the Commission in their impact assessment as regards Option 2, which is somewhat similar to this "business as usual" option. "Keeping the same budget level for the period after 2012 would not allow the Agency to perform all its functions satisfactorily…".

With no increase in staff, the budget is trivial to project (see Table 6). In order to facilitate cross comparison, the budgetary estimates in this section generally follow the same logic that the Commission used. For the most nearly corresponding Option, the Commission assumed current budget plus 2% per year inflation.

Table 6: Staffing and budget estimate for Option 2

Overview of budget under OPTION 2					
	Budget 2012	**Budget 2013**	**Budget 2014**	**Budget 2015**	**Budget 2016**
Administrative staff	20	20	20	20	20
Operational staff	37	37	37	37	37
TOTAL	57	57	57	57	57
Total expenditure					
Total expenditure	€ 8,622,080	€ 8,796,160	€ 8,965,489	€ 9,144,799	€ 9,327,695

Source: Study team

5.3.3. OPTION 3a: Enhanced resources

Most decisions about ENISA's future role have little relevance to an impact assessment. Its role will evolve, with decisions being taken annually through the Work Programme based on then-current needs. Many decisions about operational improvements are fairly clear, and should be undertaken under all Options. Thus, the primary dimensions in which to vary an impact assessment are in terms of (1) resources and (2) those aspects of efficiency where the right answer are less obvious.

To the extent that ENISA is undertaking activities that are not operational, it is difficult to say exactly what the right level of staffing should be. There is no specific activity that would necessarily cease if ENISA has too few resources. Having less-than-optimal coordination has subtle effects, and imposes costs that are difficult to quantify.

As noted in Section 5.3.2, there is good reason to believe that ENISA's staffing is less than optimal today. In fact, there is good reason to believe that it has been too low for years. Thus, option 3a concentrates on simply increasing resources.

This option attempts a rapid ramp-up of staff size in order to reach critical mass. It assumes exactly the same mandate as in Option 2, differing only in terms of staffing levels. Given that ENISA's workload is already increasing, the staff ramp-up begins in 2012; however, recognising that there is budget pressure during the current MFF period, the ramp-up is not as fast as optimal.[154]

[154] The Commission's impact assessment notes that increases in headcount are particularly challenging to achieve prior to 2014 (when the next MFF comes into play). "The estimations for the budgetary requirements for the Agency are provided for a period of 5 years (2012-2016). As regards 2012 and 2013, the budget estimations for the different options are aligned with the amounts set in the financial framework. This poses certain constraints, since the maximum allowed margin for deviation from the financial framework is 10%. Therefore, the actual implementation and impact of those policy options which foresee extension of the tasks of the Agency, and respectively of its resources, would start only in 2014. This would mean a dynamic evolution of resources between the estimated situation in 2013 and the targeted situation at the end of 2016 …", page 36.

Table 7: Staffing and budget estimate under Option 3a

Overview of budget under OPTION 3a					
	Budget 2012	**Budget 2013**	**Budget 2014**	**Budget 2015**	**Budget 2016**
Administrative staff	22	24	26	30	30
Operational staff	41	48	57	69	69
TOTAL	**63**	**72**	**83**	**99**	**99**
Total expenditure					
Tifle 1 – Staff expenditure (including recruitment expenditure)	€ 5,936,341	€ 6,968,692	€ 8,266,335	€ 10,101,831	€ 10,303,868
Tifle 2 – Costs associated to the functioning of the Agency	€ 571,236	€ 635,019	€ 713,912	€ 828,198	€ 841,035
Tifle 3 – Costs related to operational activities	€ 3,253,789	€ 3,801,856	€ 4,490,123	€ 5,465,015	€ 5,572,452
Total expenditure	€ 9,761,366	€ 11,405,567	€ 13,470,370	€ 16,395,044	€ 16,717,355

The increase in staff is in excess of the 10% guideline, but nonetheless restrained during the years 2012-2013.

The budget is computed using roughly the same assumptions as the Commission for the corresponding cases. Salary is initially € 90,659 for operational staff and € 55,906 for administrative staff. These salary levels are assumed to increase 2% per year. Title 1 is computed by adding approximately 20% to the Chapter 11 salaries computed on this basis. Title 2 costs are assumed to be roughly €186,000 plus €6,100 per staff member. Title 3 expenses are assumed to represent one third of total expense.

We assume that, with work, the ratio of non-administrative staff to total staff might be raised somewhat above current levels; however, given that the 2007 average for agencies of between 75 and 150 employees was 67%, we think that assuming more than 70% is probably unrealistic in the this time frame. Our figure thus differ slightly from corresponding Commission estimates. One should strive for continuous improvement, of course, but one should not assume it in budgetary planning.

Under this Option, staff is adequate to enable ENISA to tackle a significantly larger number of issues.

We suspect that this Option may be lacking in realism. It possibly calls for a rate of budget increase that is unacceptable;[155] however, for precisely this reason, it serves as a useful point of comparison.

5.3.4. OPTION 3b: Enhanced resources and efficiency

This Option is inspired by the same considerations as Option 3a. ENISA's mandate is the same, most circumstances are the same. Under this Option, a number of possibly more controversial efficiency measures are undertaken. By improving staff efficiency, the agency can defer some staff increase and still increase its achievements.

[155] There might also be challenges in recruiting this many new highly skilled staff into Heraklion this quickly, for reasons noted in Section 3.3.3.8.2.

In this Option, we assume that ENISA implements:

- A liaison office in Brussels, staffed with three senior professionals and an office manager;
- A branch office in Athens, staffed by eight professionals and two administrative staff.

We assume that both actions are taken in 2012. They are not incompatible with the 2004 ENISA Regulation; they are not incompatible with the Council's Decision to locate the agency in Greece; and so far as we can see, they are not fundamentally incompatible with the Seat Agreement.[156]

Once again, the budget assumptions (see Table 8) are generally consistent with those used in the Commission's impact assessment. It could be argued that one should apply corrections to address (1) higher office space costs in Brussels and possibly in Athens, and (2) reduced travel expenses. We think that it is more realistic to stick with the estimation formulae used by the Commission, because (1) as the Commission notes, they are averages across multiple agencies, (2) doing so is conservative inasmuch as the travel cost savings clearly exceed any office space costs, (3) the level of administrative overhead is not significantly different under this Option, (4) keeping the same approach again facilitates cross comparison, and (5) last but not least, we do not believe that ENISA would in practice take any savings achieved as a cost reduction. ENISA would likely choose to effectively reinvest any savings, running more missions with the same skilled staff.

Table 8: Staffing and budget estimate under Option 3b

Overview of budget under OPTION 3b					
	Budget 2012	**Budget 2013**	**Budget 2014**	**Budget 2015**	**Budget 2016**
Administrative staff	21	22	23	25	30
Operational staff	40	43	47	55	69
TOTAL	**61**	**65**	**70**	**80**	**99**
Total expenditure					
Tifle 1 – Staff expenditure (including recruitment expenditure)	€ 5,760,463	€ 6,277,001	€ 6,925,083	€ 8,129,569	€ 10,303,868
Tifle 2 – Costs associated to the functioning of the Agency	€ 559,017	€ 591,397	€ 631,280	€ 705,013	€ 841,035
Tifle 3 – Costs related to operational activities	€ 3,159,740	€ 3,434,199	€ 3,778,181	€ 4,417,291	€ 5,572,452
Total expenditure	€ 9,479,220	€ 10,302,598	€ 11,334,544	€ 13,251,872	€ 16,717,355

Under this Option, staff is once again adequate to enable ENISA to tackle a significantly larger number of issues.

[156] Seat Agreement between the Government of the Hellenic Republic and the European Network and Information Security Agency, Heraklion, 22 April 2005.

5.3.5. OPTION 4: Slight expansion of the ENISA's functions

Option 4 is a more radical option. As previously noted, the European institutions have launched a planning process that could lead to establishing a full–scale CERT for the EU institutions. ENISA is already part of this *pre-configuration team* that is driving this planning process.

Option 4 takes all parameters of Option 3b as a base, and adds to them the additional responsibility of running the CERT for the EU institutions. It thus assumes the same mission as in Options 2, 3a, and 3b, plus the additional task of operating the CERT, and a level of staffing that (for tasks other than the CERT) is generally in line with Option 3b.

There is, we think, a strong tendency to assume that ENISA is not a candidate for this role because (1) it has no operational responsibilities, and (2) it is located in Heraklion, while many of the EU institutions are located in or near Brussels.

As noted in Section 4.2.3, not all operational responsibilities are the same. Some are suitable for ENISA, while others are not. We think, notably, that there are compelling arguments that ENISA should not take on operational responsibilities that overlap those of the Member States (the Criterion 4 column in Table 3 in Section 4.2.3). On the other hand, ENISA is already in the process of stepping up to storing and analysing security breach reports, as required under Article 13a of the Framework Directive under the revised regulatory framework. ENISA has already embarked on a small activity that corresponds to the Criterion 1 and perhaps the Criterion 2 columns of Table 3 (which entail dealing with data that may have security or individual privacy implications).

This responsibility of operating a CERT for the EU institutions is intermediate. It implies 24x7 mission-critical operation; however, it does not overlap any Member State activities. There is no subsidiarity issue here. It corresponds to the Criterion 3 column of Table 3 in Section 4.2.3. We do not feel that it is inappropriate for ENISA to take on Criterion 3 operational tasks, for reasons that we explained in Section 4.2.3; however, the cost of doing so should be carefully weighed against the benefits.

Operating the CERT for the European institutions would imply the need for many things that ENISA does not have, or does not do, today, including a three shift operation, an escalation path, a higher level of internal ICT security, security clearances for staff, and more. All of these are worrisome; however, they are worrisome for whatever agency takes on this task.

We are not aware of a European agency that has exactly the right mix of capabilities to run the CERT for the European institutions. If the capability had to be set up in a new agency, or in an existing agency that does not already have the right capabilities, then the costs that would be incurred might be similar to those that would pertain for ENISA in any case.

We have included a rough budgetary estimate for Option 4. We assume, based on comparison of various national CERTs, that a professional staff of about 15 would be required, with a modest administrative staff of 3. This staffing level is consistent with a basic CERT that deals with notifications and early warning. We assume that the present pre-configuration effort, which in effect constitutes a prototype of the CERT, will remain in place through 2012, and that fully operational 24 x 7 staffing would be assumed by ENISA in 2013.

One could choose instead to implement a more comprehensive CERT that includes extensive ability to analyse incidents. This would likely require a total professional staff size of roughly 40 (plus a corresponding administrative headcount).[157] This is a perfectly viable alternative option, but it is not the one that we assumed in our budgeting.

Our understanding is that, as a practical matter, the staff for this function would have to be based in Brussels. It is perhaps unusual but not unheard of for a decentralised agency to have operations at locations other than the Seat – consider, for example, EUROPOL's Member State liaison offices, or ERA which has its headquarters in Valenciennes but its international conference facilities in Lille.[158]

Table 9: Staffing and budget estimate under Option 4

Overview of budget under OPTION 4					
	Budget 2012	**Budget 2013**	**Budget 2014**	**Budget 2015**	**Budget 2016**
Administrative staff	21	25	26	28	33
Operational staff	40	58	62	70	84
TOTAL	**61**	**83**	**88**	**98**	**117**
Total expenditure					
Tifle 1 – Staff expenditure (including recruitment expenditure)	€ 5,760,463	€ 8,146,787	€ 8,832,264	€ 10,074,894	€ 12,288,100
Tifle 2 – Costs associated to the functioning of the Agency	€ 559,017	€ 703,567	€ 745,693	€ 821,715	€ 960,071
Tifle 3 – Costs related to operational activities	€ 3,159,740	€ 4,425,177	€ 4,788,979	€ 5,448,304	€ 6,624,085
Total expenditure	€ 9,479,220	€ 13,275,532	€ 14,366,936	€ 16,344,913	€ 19,872,256

There are numerous considerations that would have to be weighed against any benefits. It is far too soon to fully elaborate this Option. The creation of the pre-configuration team was publicly announced just a few days ago, on 10 June 2011.[159] The pre-configuration team is supposed to spend the next year planning for possible implementation of such a CERT. There are a great many unknowns.

As the planning process goes forward, the best place for running the CERT will be determined. For now, however, it is useful as an illustration of one possible evolutionary direction for ENISA.

5.4. Overall assessment

In an impact assessment, it is customary to compare the options in terms of effectiveness, efficiency, and coherence with overall European goals. Direct costs are certainly also relevant.

[157] This estimate of professional staff size is consistent with the Commission's impact assessment.

[158] Ramboll et al., Evaluation of the EU decentralised agencies in 2009, December 2009, op. cit.

[159] Cyber security: EU prepares to set up Computer Emergency Response Team for EU Institutions, http://europa.eu/rapid/pressReleasesAction.do?reference=IP/11/694.

An impact assessment serves to inform policymakers; however, it is important to remember that the eventual decision is ultimately political. Bearing that in mind, there are a few observations that we would like to offer:

- Option 1 saves the expense of ENISA, but also foregoes all of the benefits. We judge this to be unwise.
- Option 2, which continues the programme as it is, retains current benefits at current cost, but does not provide the capacity needed for ENISA to expand its role, as it inevitably will. Current action lines would likely have to be curtailed over time to enable new action lines to be initiated.
- Option 3a expands staffing rapidly, enabling ENISA to take on additional tasks, and to better serve those that it already has.
- Option 3b expands staffing, but not as rapidly as 3a. At the same time, it implements overdue efficiency improvements, including a Brussels liaison office and an Athens branch office, thus enhancing the missions per professional per year, and facilitating recruiting as well. The intent is to serve the same needs as Option 3a, but with greater efficiency and thus with lower cost. The needs may be served somewhat better as well to the extent that ENISA can scale operations better so as to conduct significantly more missions (implying slightly higher effectiveness as well).
- Option 4 builds on Option 3b by adding responsibility for a CERT for the EU institutions to ENISA's mandate. It appears to be a feasible option. It is perhaps premature to assess the overall impacts of Option 4 at this time. The arguments for and against it are complex.

Table 10: Overall assessment of options

	1 No programme	2 Baseline	3a Increase resources	3b Increase resources and efficiency	4 Implement a CERT for the European instituions
Effectiveness	−−	0	+	+ / ++	?
Direct costs	++	0	−−	−	?
Efficiency	0	0	+	++	?
Coherence	−	0	0	0	0
Overall assessment	**−−**	**0**	**0**	**+**	**?**

0 = no change; **+** = better ; **++** = much better ; **−** = worse; **−−** = much worse

Source: Study team

Figure 13 and Figure 14 compare the options in terms of their implications for total staff size and total budget.

In evaluating the budget for Option 4, one should bear in mind that if a CERT for the EU institutions moves forward (as we think it should), the staffing and the associated costs will need to be carried somewhere, whether with ENISA or with some other entity. We also note once again that the decisions about what this CERT should do and how it should do it are being developed among the European institutions and within the pre-configuration team, not by this study. We are sketching a possible budget here solely to promote discussion.

Figure 13: Total staff under each option

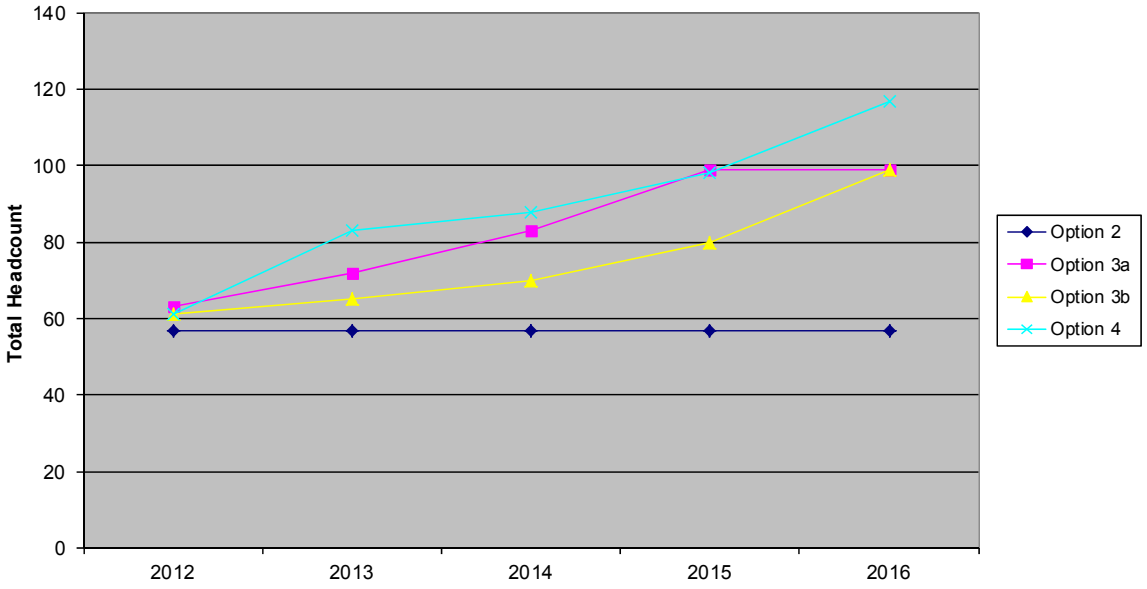
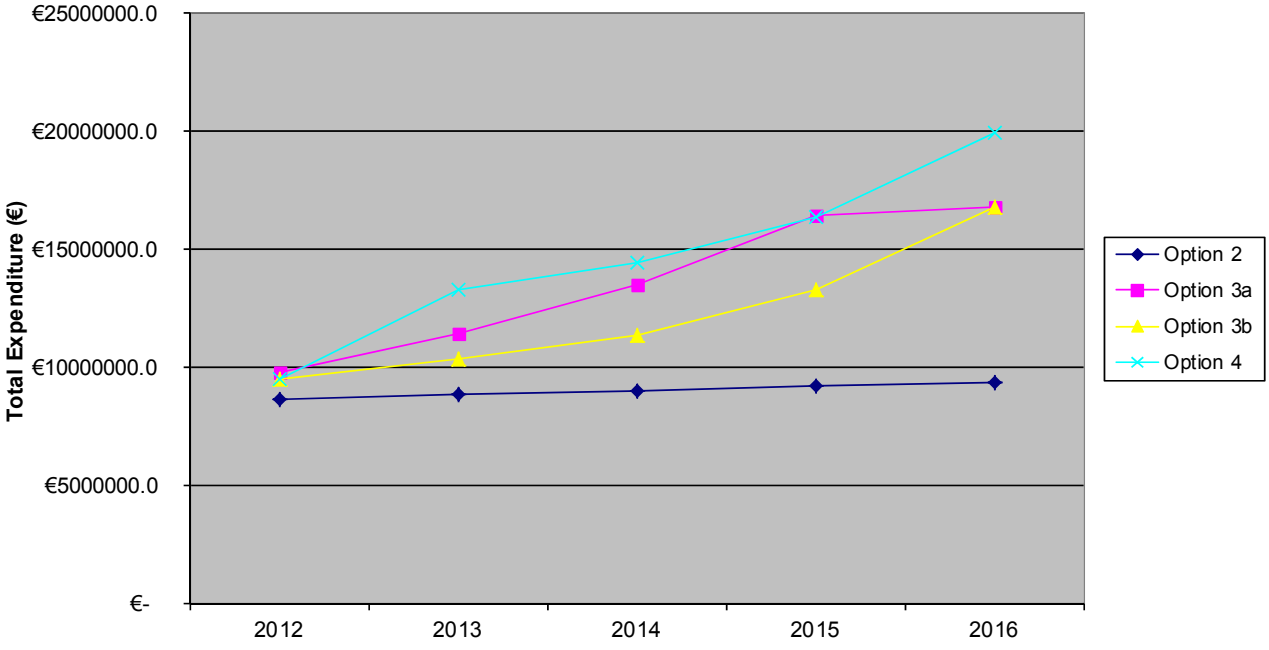


Figure 14: Estimated budget under each Option



6. CONCLUSIONS AND RECOMMENDATIONS

Recommendations appear at the point in the text at which they are most relevant. The table below provides pointers to all of them. The remainder of this chapter then provides a brief recapitulation of each recommendation.

Note that the recommendations take today's reality as their baseline. Some of these recommendations are addressed in the Commission's proposed new Regulation, while others are not.

ENISA should be subject to a fully independent evaluation not less frequently than twice per Multiannual Financial Framework (MFF) cycle.[160] This would put it on the same calendar as many other European agencies.

The last fully independent evaluation of the agency was completed in 2007, based on data collected late in 2006, which is to say that it is four and a half years old. In a more typical cycle, an agency would be reviewed twice per seven year MFF cycle, in which case the evaluation data could never be as stale as in this case.

Any revision of the ENISA Regulation should state affirmatively what the mission of the MB is, and clarify its role relative to that of the Executive Director.

The 2004 Regulation may have under-specified the MB's mission, thus opening the door to disputes. We are advising clarification, but not major changes.

[160] The current MFF cycle ends in 2013. The next runs from 2014-2020.

Any revision of the ENISA Regulation should formalise the MB's role in strategic staff planning.

Since this was historically a point of contention, clarification is in order. We see no need for a substantive change.

Ensure that the MB has access to independent legal and staff resources when required, especially in regard to personnel matters. Consider making similar support available to all of the decentralised agencies.

In most cases, the MB can rely on ENISA resources. In rare instances, this is inappropriate.

A new regulation for ENISA should either (1) not limit the time period for which it is established, or (2) align its period of establishment with the next Multiannual Financial Framework (MFF) cycle (2014-2020).

We feel that it is now well established that ENISA meets real needs at European level, and that an independent agency is the appropriate vehicle for meeting those needs. At a minimum, ENISA's period of establishment should be aligned with the MFF cycle.

The scope, tasks and objectives in the Regulation should be revised so as to reduce ambiguities and reduce the risk of misinterpretation; however, reduction in ambiguity should not be achieved at the expense of needlessly increasing the rigidity of the revised Regulation in comparison with that of the current Regulation.

In our view, the flexibility of the 2004 ENISA Regulation has enabled ENISA to move appropriately into a number of new areas where it adds substantial value. This is a valuable property that should be preserved in any revision.

Explore ways to systematically exchange best practice among the decentralised European agencies in regard to efficient implementation of administrative procedures.

There seems to be huge variation among small decentralised agencies as to the degree of administrative overhead required. There could be merit in creating overall lightweight mechanism to encourage the exchange of best practice among the decentralised agencies.

ENISA should open a small Brussels liaison office as soon as practically feasible.

Given the large number of trips to Brussels, the argument for a Brussels liaison office is compelling – not only as a means of saving cost, but also as a mean of enhancing the

effectiveness of ENISA. There is ample precedent among decentralised agencies for a Brussels liaison office. We see no need to wait for a revised ENISA Regulation – so far as we can see, subject to availability of budget, this is within the decision authority of ENISA's management and MB.

ENISA should seriously consider assigning personnel on a long term basis to a branch office in Athens, subject to reaching suitable understandings with the host country government.

There is also a strong argument, primarily based on travel efficiency but also on recruiting and retention considerations, for opening a branch office of suitable size at a location with much better travel connections than Heraklion. Athens is the obvious candidate. We believe that this could, under suitable conditions, be launched prior to a new ENISA Regulation coming into force.

Senior management of FORTH and ENISA should task a small committee of their respective experts to explore whether there might be additional synergies between the two organisations. The committee's report should be made available to the ENISA MB.

ENISA and FORTH (a research institute with relevant capabilities, and ENISA's host in Heraklion) already cooperate in a number of areas, but we think that the potential for synergies has not yet been fully explored.

Any revision of the ENISA Regulation should clarify ENISA's ability to engage with privacy and data protection stakeholders, to enable ENISA to support these activities, subject to due respect for the principle of subsidiarity.

The 2004 ENISA Regulation places limitations on ENISA's ability to engage with cybercrime and with privacy / data protection; however, this has not prevented ENISA from engaging actively, effectively and appropriately in these areas. Clarification would be in order. Clarification of its relationship to the military might also be beneficial.

Consider seriously increasing ENISA's budget and staffing so as to enable it to engage more extensively with industry and consumers, global counterparts, and standards bodies.

In the nature of what ENISA does, there is no way to rigorously identify a "right" number of staff, but we have a strong sense that the current staff level is less than ideal for addressing the many issues that are best and most appropriately handled by ENISA. Any staff increase should be undertaken as part of balanced programme that also seeks improvements in efficiency and effectiveness.

EUROPEAN PARLIAMENT

DIRECTORATE-GENERAL FOR INTERNAL POLICIES

POLICY DEPARTMENT A
ECONOMIC AND SCIENTIFIC POLICY

Role

Policy departments are research units that provide specialised advice to committees, inter-parliamentary delegations and other parliamentary bodies.

Policy Areas

- Economic and Monetary Affairs
- Employment and Social Affairs
- Environment, Public Health and Food Safety
- Industry, Research and Energy
- Internal Market and Consumer Protection

Documents

Visit the European Parliament website: **http://www.europarl.europa.eu/studies**

PHOTO CREDIT: iStock International Inc.

ISBN