National-level Risk Assessments

An Analysis Report

November 2013

European Union Agency for Network and Information Security www.enisa.europa.eu

About ENISA

The European Union Agency for Network and Information Security (ENISA) is a centre of network and information security expertise for the EU, its Member States, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU Member States in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU Member States by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Authors

Panagiotis TRIMINTZIOS

Razvan GAVRILA

Contact

For information about this work please use: c3e@enisa.europa.eu

For media enquires about this report, please use press@enisa.europa.eu

Acknowledgements

The analysis in this report was produced in collaboration with RAND Europe. ENISA would like to thank Neil Robinson, Tess Hellgren, Kate Robertson, Lucia Muchova of RAND Europe, and Peter Burnett of Quarter House Ltd. This study would not have been possible without the extremely useful input by the experts who were interviewed from the organisations that participated in the study (the list is available in *Annex A: List of organisations involved in the study* (p.35); we are grateful to all of them. Authors' would also like to thank their colleague Dr. Louis Marinos for his useful and constructive feedback.

Executive summary

This report is based on a study and analysis of approaches to national-level risk assessment and threat modelling for cyber security which was conducted between April and October 2013. ENISA aims to provide an evidence-based methodology for establishing a National-level Risk Assessment in order to contribute to the wider objective of improving national contingency planning practices (NCPs)[1]. This report will help towards rationalising national risk assessments in EU Member States in order to reduce or eliminate vulnerabilities of critical Information and Communication Technology (ICT) services and infrastructures. This objective was articulated in the February 2013 European Cyber Security Strategy and thus sits within broader EU-wide efforts to improve crisis cooperation activities.

This report should be of use to policy-makers who are charged with implementing a CIIP or cyber security risk assessment programme. In addition, other interested parties may include regulators, researchers and senior industry representatives from Critical Information Infrastructure sectors.

In this study we have analysed current National-level Risk Assessment practices in around twenty countries and tried capture the main aspects of the implementation of their National-level Risk Assessments. Which of these aspects are most effective in a particular country depends to a certain extent on important administrative, economic, legal and cultural factors such as the dependence of society on cyberspace; the way in which government activities are conducted and the pre-existing state of the art in information security risk management. It is also important that National-level Risk Assessment programmes should be linked to a national cyber security strategy. A high-level cyber security strategy, clearly owned, can provide the context and ultimate rationale for a National-level Risk Assessment programme.

There are a number of permutations or variations in National-level Risk Assessment which may be implemented depending on the specific context of the country. Such possible options have been listed in this report, with clear guidelines for National-level Risk Assessment programme manager on how to identify these local specificities and requirements.

Regarding the identification of threats and modelling we have found that the most important are:

- articulated in a high-level strategy,
- based on scenarios,
- described qualitatively or quantitatively.

Concerning approaches to the conduct of a National-level Risk Assessment, they can be performed:

- through a formalised central framework or approach (a one-size-fits-all), or
- based on a decentralised model where each actor prepares their own risk assessment to be integrated by a coordinating authority.

Finally, national-level risk management methodologies may be based upon:

- Scenario-based approaches where actors are gathered together to consider scenarios in the round; such scenarios describe risks as a narrative and label them by applying simple categories of likelihood and impact (low, medium, high),
- Quantitative approaches which apply ordinal thresholds (e.g. a risk is classed severe if it affects 1 in 20,000), or
- Approaches which combine elements of all of the above (for example, using scenarios and then qualitative and quantitative methods).

[1] For more on this topic see ENISA's Guide for National Contingency Plans: http://www.enisa.europa.eu/c3e/national-contingency-plans

Key challenges

We have identified a number of key challenges for National-level Risk Assessment programmes, including:

- The lack of a harmonised national framework for cyber security, particularly with regard to terminology;
- Incomplete and diverse risk assessment methodologies (especially in the pan-European context);
- The lack of comprehensive methods to address threats;
- The need for effective risk management and preparedness capacity and skills;
- The need for more information sharing between different actors involved in a National-level Risk Assessment

Common lessons

The lessons learned are grouped into the following areas:

- The need to leverage international best practice, as many countries had visited others to learn about risk analysis practices;
- The importance of establishing effective collaboration between the public and private sectors, especially where in some cases the private sector owns considerable parts of the infrastructure;
- Finally, the need for effective critical information infrastructure approaches to be tailored to each national context.

Current priorities of National-level Risk Assessment programmes

Countries reported that they were focusing upon a number of priorities in the near to medium term, including the following:

- Improving understanding of threats and their effects upon society;
- Better incident management;
- Greater stakeholder involvement and information sharing;
- Improved national CIIP frameworks;
- Seeking further EU guidance and support.

In conclusion we can see that understanding of the national approach to cyber security and how risk decisions are taken in different countries is important to ensure that the results of any National-level Risk Assessment reach key decision-makers at the right time. It is also clear that there are a variety of approaches and levels of sophistication used in National-level Risk Assessments. **Qualitative** tools appeared to be preferred due to the complexities of understanding risk in the cyber domain. Depending on the preconditions regarding implementation, risk assessment could be performed using a **common set of methods** or in a more **decentralised fashion**. Challenges included the **diversity of methodologies** and approaches to National-level Risk Assessments (which highlights the need for this guidance document) as well as the complexities of **public–private cooperation**. As might be expected, many countries studied drew lessons from others when preparing their National-level Risk Assessment programmes. Some countries had identified priorities that they were seeking to focus on, including greater understanding of threats, improved stakeholder engagement and better national CIIP frameworks.

Recommendations

Based on an analysis of the data gathered we recommend the following:

1. Member States should understand better the underlying cyber threats and risks that they face and the impact to society.
2. Member States are advised to integrate National-level Risk Assessment into the lifecycle of NIS incident management and cooperation plans and procedures.

3. Member States should expand public–private sector dialogue and information sharing.
4. A practical step-by-step guide on how to perform National-level Risk Assessments should be developed, tested and maintained. Such a guide should be piloted by countries at the early stages of preparing their own National-level Risk Assessment programme. ENISA or another international institution would be appropriate bodies to oversee this action.
5. A catalogue of scenarios to help Member States in their National-level Risk Assessments should be established at EU level. Such a catalogue could be based on work already being done at ENISA on the threat landscape[2] and incident reporting[3].
6. The EU community of practitioners with an interest in cyber National-level Risk Assessments should be established and strengthened as information exchange platform, e.g., within the framework of the European Commission's NIS Platform[4].
7. Risk analysis expertise must be shared from other domains that assess complex cross-border risks, such as border security, financial services, aviation or public health for example within the European Commission's NIS Platform and other activities organised by ENISA.

[2] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment
[3] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
[4] http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

Table of Contents

1 Introduction

> *The capacity to manage crises is a fundamental element of good governance, as it tests governments' capacity to provide the right responses at the right time to protect their citizens and businesses and mitigate the impact of disasters.*[5]
>
> *Effective risk assessment methodologies are the cornerstone of a successful Critical Infrastructure Protection programme.*[6]

This chapter introduces the topic of risk assessment and provides a rationale for why this guidance is required.

We lay out some broad challenges associated with the areas of threat modelling and risk assessment as they relate to a wider range of efforts to strengthen Member States' activities on cyber[7] crisis management and cooperation, cyber contingency planning, cyber exercises and – more specifically – the role that National-level Risk Assessments play in mitigating and reducing Critical Information Infrastructure (CII) vulnerabilities. Although threats and impact are important, in the context of risks, but also there are some other ones like: asset identification, assets valuation, risk prioritization, scope of the assessment, assumptions made, experience from incidents, protection level from current controls, gap analysis, risk appetite, etc. These are the main grounds for diversification in risk assessments.

Risk assessment and management in particular is important to prevent, as well as manage, crises since it lays the groundwork for effective crisis response. Undertaking risk analysis prior to a major incident that might lead to a crisis makes it more likely that the response will be effective and efficient.

1.1 Purpose of this report

This document is an Analysis Report containing the core evidence base from a study to understand the practice of National-level Risk Assessments in different countries. The document is accompanied by a Step-by-Step Guide on how to perform National-level Risk Assessment that contains more practical guidance intended for implementation. These two documents are thus complementary: the analysis report contains essential background information necessary to understand the context prior to engaging on practical implementation using the Step-by-Step Guide. **Target audience**

This report is of use to policy-makers at national and international levels who are charged with implementing a CIIP or cyber security risk assessment programme. Other interested parties may include regulators, researchers and senior industry representatives from Critical Information Infrastructure sectors.

1.1.2 About this document

Chapter 1 introduces the topic and provides a rationale for why this guidance is required.

[5] *Opening remarks by OECD Deputy Secretary-General Yves Leterme at the Joint OECD–Swiss federal Chancellery Workshop on Inter-Agency Crisis Management 28 June 2012, Geneva, Switzerland available at http://www.oecd.org/governance/risk/Speech%20DSG%20Leterme%20-final.pdf*

[6] Giannopoulos G, Filippini, R and Schimmer, M (2012) Risk assessment methodologies for Critical Infrastructure Protection. Part 1: a State of the Art JRC Technical Notes EUR 25286 EN-2012 Ispra, Italy

[7] The World Economic Forum defines 'cyber' as referring to the interdependent network of information technology infrastructures, and includes technologies such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries (WEF 2012).

Chapter 2 provides an overview of the context including the policy landscape and guidance developed by ENISA in the context of National-level Risk Assessments.

Chapter 3 presents a detailed summary of the findings.

Chapter 4 provides some conclusion and recommendations.

This is followed by an extensive bibliography and list of acronyms used in the report.

Appendices contain a list of participating countries, the questionnaire and Key Informant Interview (KII) protocol used in the study.

1.2 Understanding risk assessment – terminology

'Risk' is usually defined as the potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization[8]. Haimes (2004) defines 'risk' as a 'measure of the probability and severity of adverse effects' and notes that it is difficult to comprehend because:

> *it is a complex composition and amalgamation of two components – one real (potential damage or unfavourable adverse effects and consequences), the other an imagined mathematical human construct termed probability.*

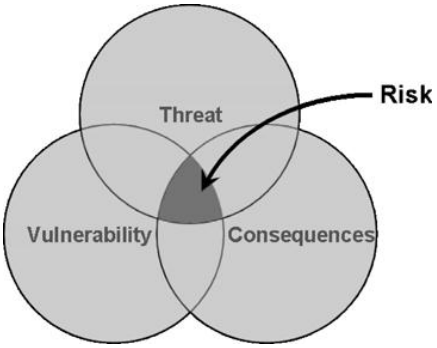


Figure 1: Risk definitions[9]

The following definitional questions , raised by Willis, should be answered prior to embarking upon a risk assessment:

- **Security** – how broadly is security defined? Does it relate to national security or a wider interpretation perhaps including safety (e.g. energy security)?
- **Threat** – does the threat model define directed threats (e.g. including a classification of different adversaries or agents such as organised criminal groups, nation-states etc.) or non-directed threats (e.g. accidents, hardware or software failures)? Does it include systemic concerns such as natural disasters? How dynamic is the threat model?

[8] ISO/IEC 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
[9] Based on Willis 2007.

- **Vulnerability** – what characteristics of the domain, asset or infrastructure are vulnerable or provide opportunities for the realisation of risk?
- **Impact** – is impact defined in primary or secondary approaches? For example, would it cover the long-term secondary consequences of the realisation of a risk or the consequences of aversion measures?
- **Asset definition –** what are the approaches used to identify the critical assets, required for an organisation's operations and their continuity, including Information resources that support the organization's mission?
- **Likelihood –** what are the approaches used to measure the probability that a specific event will occur? Will this model incorporate uncertainty?

A distinction is often made between risk analysis (or risk assessment) and risk management (i.e. the implementation of measures to address the risk identified, which might be to avoid, reduce, share or retain the risks) (Dorfman 2007).

Definitions used in a particular risk assessment will need to take into account that, from an operational perspective, it may be possible to significantly reduce a risk (rendering the chances of it occurring infinitesimally small), but that statistically it may not be possible to eliminate it entirely.

1.3 About risk assessment

During our research on risk assessment, both in the context of studies into risk generally and those focusing on national security, we have identified four main issues that are applicable to CII risks:

- Risk assessment is designed to increase awareness of the different kinds of risks that may have an impact on CII specifically and national and EU security in general.
- Properly understanding risk assessment enables us to identify key risks and their primary drivers as well as to collect the most appropriate data to quantify those risks and their consequences.
- Considering the diversity of the EU Member States' preferences and approaches to measuring risks, identifying the methods used in each Member State is a vital first step towards greater harmonisation, collaboration and effectiveness in managing resource deployment and planning for the future. Different approaches should aim towards similar outcomes and this is achievable by finding common recipes in using different tools to achieve common results.
- Collecting different types of risk assessment and analysis methods used by Member States allows the identification of best practices and common challenges.

1.3.1 Strategic challenges in conducting risk assessments in general

A number of high-level challenges to risk analysis may be identified, which are present regardless of the domain of risk. The ability to analyse different types of information from diverse stakeholders is among the core challenges that risk analysts in any domain may confront. Choosing the right method(s) of risk analysis is also one of the challenges. Depending on the type of risks assessed, different methods may be employed, including the range of participatory methods that include surveys, focus groups and expert panels (see Willis et al. 2004). Deciding on the appropriate risk assessment and risk management strategy also requires careful analysis of the available data. Finally, there is concern over terminology and the meaning of different terms.

1.3.2 Important operational questions specific to CII risk assessments

From an operational perspective, practising risk analysis also raises several other important questions pertinent to the specific application of risk analysis and which may be specific to the particular domain of CII and cyber risk. Only those involved in implementing a National-level Risk Assessment programme will be able to provide suitable answers to such questions. These questions include:

(1) How can risk be estimated?

(2) What are tolerable levels of risk?

(3) Should (and if so how could) resources be allocated based on risk analysis?

For example, relating to the first question (with a specific focus on cyber security) Sandia Labs in 2012 released a report into Cyber Threat Metrics which attempts to list cyber threats and measure them consistently and unambiguously (Mateski et al. 2012).

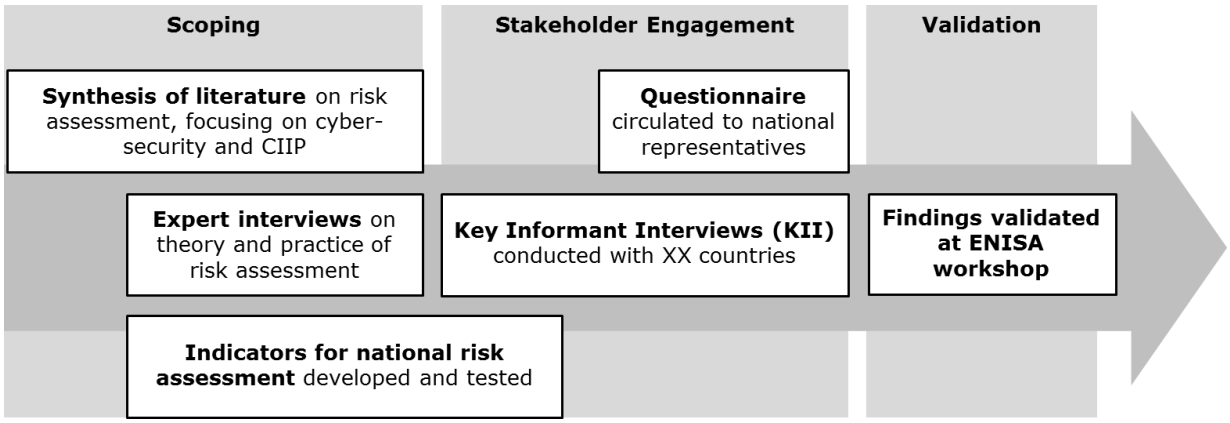
Relating to the second issue, Willis et al. (2012) discuss risk preferences in the Dutch national risk assessment model. These preferences are used to determine what 'weight' citizens appear to place on different levels of risk and therefore what they might consider tolerable or not.

Regarding the allocation of resources in the area of border security, it has been found that changing the pattern of risk management measures (border patrols and so on) has a demonstrated effect upon risks. Using pattern analysis has been proven in an experimental setting to improve metrics for risk management such as higher interdiction rates for illegal border crossing[10]. Note that this is tool or method independent. So this means that the method and/or tool is not the key.

1.4 Methodology

1.4.1 Overview of methodology

This report summarises results from a study conducted between April and October 2013. Figure 2 illustrates the steps taken during the study.



[10] Predd, Joel B, Henry H Willis, Claude Messan Setodji, Chuck Stelzner (2012). 'Using Pattern Analysis and Systematic Randomness to Allocate U.S. Border Security Resources'. Santa Monica, CA: RAND Corporation, 2012. As of 9 September 2013: http://www.rand.org/pubs/technical_reports/TR1211

Figure 2: Study design

The study consisted of:

(1) A review of policy documents, technical reports and recent scientific research papers[11], concerning risk analysis and assessment both in general and also specifically referring to cyber security and CIIP.

(2) Conducting a series of unstructured interviews with academic and governmental experts concerning the theory and practice of risk assessment. The aim of these interviews was to feed into the generation of a set of indicators by the research team of the overall level of the sophistication of national risk assessments.

(3) Testing these indicators with three national-level key informant interviews (KII).

(4) A first step was conducting interviews with 17 national key informants (see *Annex A: List of organisations involved in the study* (p.35). The organisations were selected on the basis of a pre-analysis of existing indicators relating to cyber risk analysis and indicators relating to the more generic consideration of risk. Such indicators included: standardisation of terminology, presence of a national cyber security strategy and integration of cyber security RA in national risk assessments or CII asset definition and monitoring.

These were guided by an interview protocol. The aim of these interviews was to cross-check and challenge the understanding within the study team of the key issues in national risk assessment. Each interview was conducted according to the 'Chatham House rule'[12] and interviewees were sent notes of their interview afterwards in order to verify the understanding of the study team. Interviews were mainly conducted via telephone. A copy of the interview protocol can be found Key Informant Interview Protocol.

(5) In a second step, a questionnaire was prepared which aimed to consolidate and confirm findings from the Key Informant Interviews and to gather further evidence. For those countries that had already participated through key informant interviews, a questionnaire was sent to interviewees, pre-populated with their responses for verification. Representatives from an additional four countries completed the questionnaire. A copy of the questionnaire can be found in *Annex C: Questionnaire* (p.38).

(6) A validation workshop in September 2013 at ENISA's 2nd International Conference on Cyber Crisis Cooperation and Exercises, which was held in Athens, Greece.[13]

Overall, we collected information from 21 organisations. In accordance with the Chatham House Rule, participants have not been specifically identified but the countries that participated are listed in *Annex A: List of organisations involved in the study* (p.35) while the protocol used is given in *Annex B: Key Informant Interview Protocol* (p.36).

[11] The full list of references is available in the Bibliography at the end of this report.
[12] Chatham House rule: http://www.chathamhouse.org/about-us/chathamhouserule
[13] 2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, http://www.enisa.europa.eu/activities/ccce-conference

2 Context

This section summarises policy initiatives and guidance at national, European and international level on cyber security and risk assessment. We provide an overview of the most recent and relevant policy developments in this area up to and including the revised ENISA mandate of June 2013, the February 2013 EU Cyber Security Strategy (EUCSS) and accompanying Commission proposal for an NIS Directive (European Commission 2013a).

2.1 Policy impetus in Europe

In recent years, policy-makers in Europe have been strengthening cyber security commitments and capabilities.[14] This is reflected in the formulation of a number of cyber security strategies both at European and Member State level.[15] In February 2013 the European Union released its overarching European Cyber Security Strategy with accompanying legislative proposals for a Network and Information Security (NIS) Directive. The need to focus on a more coordinated approach has been highlighted in several European Commission communications (e.g. European Commission 2009[16]), and the Commission has taken tangible steps towards creating a pan-European policy. The comprehensive European Cyber Security Strategy covers the main relevant policy domains: resilience and NIS in cyberspace, tackling cybercrime and an international strategy and defence policy with respect to cyber security.

Within the 2013 European Cyber Security Strategy, the policy mandate for improving resilience and NIS security sits with Directorate-General for Communications Networks, Content and Technology (DG CNECT) and seeks to strengthen the resilience of critical infrastructure, enhance preparedness and foster a cyber-security culture through the centralisation of information, private sector partnerships, single market-based approaches and an international outlook (European Commission 2013b).

A key element of the 2013 proposals for an NIS Directive is the broader information collection mechanism to gather information on threats and incidents.

Prioritisation of threats in the Strategy is based on lessons learned from large-scale incidents. Regular meetings of the Commission are used to determine the level of threat severity using a scale of 1–3. There is no single international categorisation on threat criticality, although ENISA published a study into threat characterisation (see below) which synthesises a range of different assessments. It goes without saying that if a large incident has happened does not mean that this is a more or less serious threat. Rather, a large scale incident bears some relevance to impact. There are also a few other elements in this than threat priorities (e.g. vulnerabilities, protection level, etc.).

ENISA has also been playing a role in supporting implementation of European cyber security policy by providing guidance on National Contingency Plans (NCPs) and National Cyber Security Strategies (detailed below).

[14] For example, a recent study found that across European countries, cyber security threats are characterised as high, major, prominent or priority when compared to other national-level risks (for example terrorism, pandemics, natural disasters, state-on-state conflict and nuclear war). See Robinson et al., forthcoming 2013.

[15] For example, Belgium, Italy and the Czech Republic have recently introduced cyber security strategies and the formulation of a European Cyber Security Strategy was released in February 2013

[16] European Commission's Communication on Critical Information Infrastructure protection (CIIP), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF

The Digital Agenda for Europe (European Commission 2010, p. 245) and the European Cyber Security Strategy emphasise the increasingly interconnected nature of threats and their impact in cyberspace, and accordingly advocate coordinated responses. The Strategy emphasises that cyber threats are not EU-specific and cannot be overcome by the EU alone; rather, they can emanate from and affect any part of the world. The 14 actions proposed in the Digital Agenda for Europe specify a number of threats, including terrorist or politically motivated attacks against information systems which form part of the critical infrastructures of the EU and its Member States.

In early 2013, ENISA published a threat landscape (ENISA 2013b), which classifies these threats according to both the vector (for example, drive-by downloads, worms, trojans, exploit kits, botnets) and threat agents. This distinction is important because it separates the ways or routes and the agent behind them. The list of threat agents is described thus:

- Corporations
- Cybercriminals
- Employees
- Hacktivists
- Nation states
- Terrorists

Outside of the specific areas of cyber security, in 2009 the European Commission also published a communication on a community approach to the prevention of natural and man-made disasters (European Commission 2009) which sets out a number of measures to be included in a community strategy for prevention of natural and man-made disasters. These measures were set out under four main headings:

- Creating the conditions for the development of knowledge-based disaster prevention policies at all levels of government
- Linking actors and policies throughout the disaster management cycle
- Making existing instruments perform better for disaster prevention
- Reinforcing international cooperation in the field of prevention

In addition, a 2010 European Commission Staff Working Paper on Risk Assessment and Mapping Guidelines for Disaster Management (European Commission 2010) illustrates how Risk Assessment can be used as a framework to aid in the management of civil contingencies.

Nonetheless, it may be observed that policy impetus revolves around three main topics:

(1) The importance of understanding and identifying the risks (risk assessment);
(2) The importance of preparedness[17] (NCPs, national exercises, pan-European exercises, pre-defined process and infrastructures);
(3) The importance of 'lesson learning' and cooperation.

2.1.1 The role of National Contingency Plans

In this section we will look at the role of National Contingency Plans (NCPs) in managing, responding to and recovering from major CII incidents.

Critical information infrastructures are vulnerable to a variety of disruptions by both man-made (where there is a directed threat, i.e., motivated adversaries who behave strategically or via human error) and systemic risks (accidents or consequences of other risks or systemic failures). High-profile

[17] For a definition and discussion on this subject please look at the Risk Preparedness paper that has been published by the ENISA Working Group on Risk Management. Available here: http://www.enisa.europa.eu/activities/risk-management

examples include the cyber-attacks targeting South Korea in early 2013; the accidental severing of submarine telecommunications cables in 2008 off the coast of Egypt and outages suffered in Syria in 2012 and 2013 and a Distributed Denial of Service (DDoS) attack against the Domain Name Service (DNS) of Network Solutions in January 2009. While such events may be reduced through effective risk management, it is virtually impossible to eliminate all risks. Successful contingency planning, execution, and testing are thus essential to mitigate the risk of system and service unavailability.

ENISA is taking important steps to further this aim: in 2011, the Agency studied NCPs in several countries and released a good practice guide.[18] NCPs are the national-level interim structures and measures to respond and recover services following major incidents that involve CIIs and that lead to a crisis. NCPs include actions at all levels, from the technical to the operational/tactical, to the strategic/political.

NCPs, also referred to as National NIS Cooperation Plans in the proposed NIS Directive,[19] are the national-level structures and measures to recover services following major crisis-inducing incidents that involve CIIs.

The European Commission recognises the importance of national contingency planning in the mitigation and recovery process, and acknowledges that this is a vital means for reinforcing EU defence mechanisms for CII. In its Action Plan[20] for enhancing the security and resilience of European CII, the Commission points out the need to develop 'national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. National/Governmental CERTs/CSIRTs may be tasked to lead national contingency planning exercises and testing, involving private and public sector stakeholders. The involvement of ENISA is called upon to support the exchange of good practices between Member States' (European Commission 2009).

Furthermore, Article 5.2 of the proposal for a NIS Directive released in February 2013 (European Commission 2013a) also articulates the way a risk assessment should fit into an overarching strategy and plan, namely that:

> *The national NIS strategy shall include a national NIS cooperation plan complying at least with the following requirements*
>
> *(a) A risk assessment plan to identify risks and assess the impacts of potential incidents;*
>
> *(b) The definition of the roles and responsibilities of the various actors involved in the implementation of the plan;*
>
> *(c) The definition of cooperation and communication processes ensuring prevention, detection, response, repair and recovery, and modulated according to the alert level;*
>
> *(d) A roadmap for NIS exercises and training to reinforce, validate, and test the plan.*
>
> *Lessons learned to be documented and incorporated into updates to the plan.*

Figure 3 illustrates the potential actors and potential structures involved in an NCP based on ENISA's good practice guide.

[18] More information is available at: www.enisa.europa.eu/c3e/nis-cooperation-plans
[19] See Article 5 of the proposed NIS directive at: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security
[20] http://ec.europa.eu/digital-agenda/en/news/policy-critical-information-infrastructure-protection-ciip

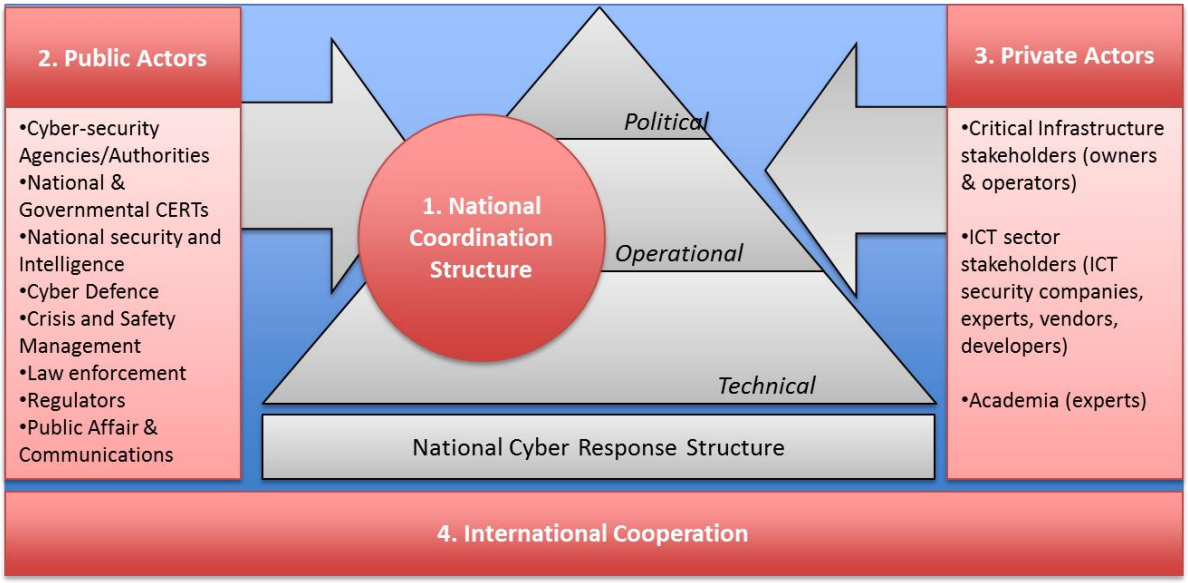


Figure 3: National NIS Cooperation Plan Structures[21]

Interim structures may involve the formation of committees and response teams (at various levels), the initiation of secure, robust means and platforms for communication, possibly the assembly of a crisis cell, and the involvement of different actors from the private sector(s) that have predefined roles during the crisis response. For managing national and cross-country large-scale cyber incidents (leading to crisis situations) it is necessary to have a proper NCP which includes international cyber crisis cooperation. NCPs include actions at all levels – ranging from the technical, to the operational/tactical, to the strategic/political.

The lifecycle of NCPs is depicted in Figure 4. Based on ENISA's previous work on NCPs, the NCP usually has a lifespan of 2–3 years depending on the size of the country and the complexity. It is clear, though, in all cases that in the development lifecycle of NIS contingency plans and their subsequent revisions the first step is to perform a thorough national NIS risk assessment. Other steps include the design and deployment of the plans, the testing, training and exercising, and finally the reviewing and auditing.

[21] Good Practice Guide for National Contingency Plans for CIIP, ENISA, 2011.

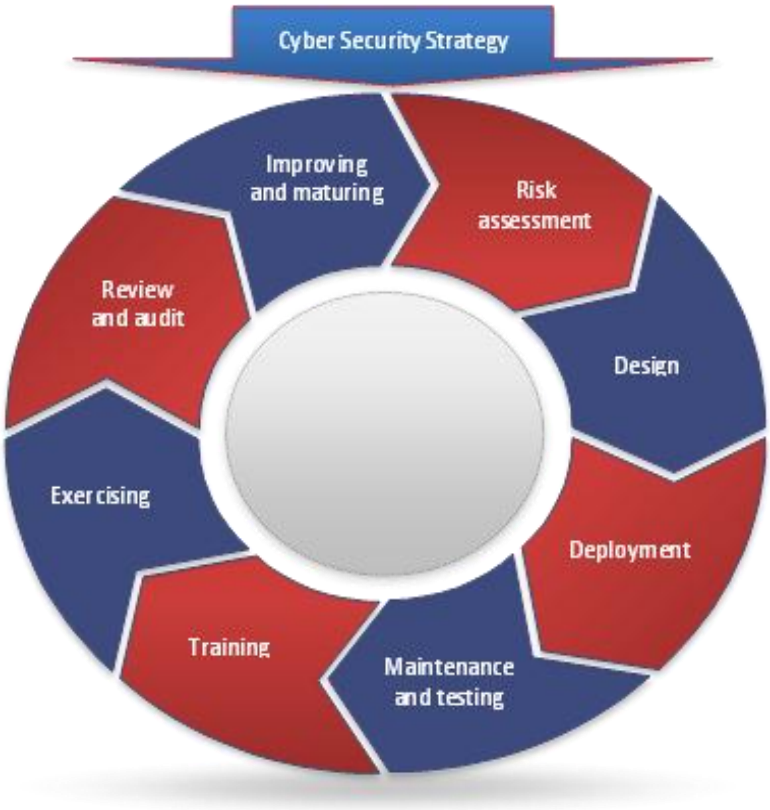


Figure 4: The lifecycle of national NIS contingency plans (source: ENISA Good Practice Guide on NCPs)

2.1.2 National policy initiatives

Across a range of EU and non-EU countries, there are some disparities in how CII / Cyber security threats and risks are characterised with a wide variety of descriptions, scope and approaches across each country (Robinson, 2013).

However, as the Impact Assessment accompanying the 2013 proposal for an NIS Directive shows, many EU countries already have efforts such as adopting a national CERT, cyber exercises or have a National Cyber Security Strategy. Nonetheless, some countries remain at a somewhat early level of maturity in this area (European Commission 2013c).

2.1.3 Examples of international initiatives on risk assessment for cyber security

In 2012 the Organisation for Economic Cooperation and Development (OECD) held a workshop on national-level crisis planning and interagency coordination in partnership with the Swiss Federal Chancellery.[22]

The key objective of the workshop was to facilitate transnational knowledge-sharing and to encourage cross-sector partnerships through identification of best practice. This objective has also been promoted through the OECD High Level Risk Forum, a venue for senior policy-makers and

[22] *Opening remarks by OECD Deputy Secretary-General Yves Leterme at the Joint OECD – Swiss federal Chancellery Workshop on Inter-Agency Crisis Management 28 June 2012, Geneva, Switzerland available at* http://www.oecd.org/governance/risk/Speech%20DSG%20Leterme%20-final.pdf

industry executives to advance the international policy agenda for building resilience to large-scale risks.

The discussions focused on improving risk management through international strategic cooperation and exchange of best practices. It also addressed the issue of governance, emphasising the importance of equipping national authorities with the right tools and institutional frameworks for coordinated action and swift responses. OECD debate has also highlighted the need to engage senior political leaders regarding investment in risk management capabilities in order to achieve practical impact.[23] Another good example of this sort is the World Economic Forum that runs a risk management exercise and delivers a risk report for the Davos meeting of political leaders. It is interesting to see how this (non NIS) based assessment is being conducted and how different voices are unified under a number of certain contexts.

2.2 The role of ENISA

Created in 2004, ENISA acts as a centre of excellence for Member States and EU institutions on network and information security issues, and has established itself as a key stakeholder in the European cyber security community. ENISA has been at the forefront of supporting the work of EU Member States and other relevant stakeholders in their efforts to develop and maintain NCPs for CIIs. The first step towards this target was the preparation of a Good Practice Guide[24] intended to shape the development process of coordinated response and crisis management of large-scale CII incidents. The Guide has helped facilitate the development of NCPs and their lifecycle, and has helped EU Member States to develop, test, improve and maintain well-functioning NCPs. Since then, the Agency has held numerous workshops across Europe to assist in the planning of national exercises to help explore and strengthen NCPs.

ENISA is working on guidance for national cyber security strategies (NCSS).[25] The Agency successfully oversaw the coordination of the first pan-European cyber security exercises[26] in November 2010, Cyber Europe 2010. ENISA facilitated the second pan-European cyber exercise, Cyber Europe 2012, which took place on 4 October 2012. As stated in the 2009 Commission Communication on Critical Information Infrastructure Protection (European Commission 2009), the 2010 Digital Agenda (European Commission 2010, p. 245) and the evaluation report of Cyber Europe 2010 (ENISA 2010), exercises are deemed an important element of a coherent strategy for cyber-incident contingency planning and recovery, both at national and European levels. It is in this context that the further investigation of threat modelling and risk assessment for CII risks takes place.

ENISA has done considerable work on Risk Management over the last years. The full information about this work can be found in a structured way at the Risk Management webpages at ENISA's website.[27]

[23] ibid
[24] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/national-contingency-plans
[25] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss
[26] http://www.enisa.europa.eu/c3e
[27] http://www.enisa.europa.eu/activities/risk-management

3 Summary of Findings

In this chapter we present a summary of our findings from the empirical research. These findings are structured according to the following broad subject areas:

- Published open guidance for RAs
- National context for cyber security
- Implementation of National-level Risk Assessment

3.1 Existing guidance on Risk Assessment

From our targeted reviews we found several high-level guidance documents concerning the process of establishing a National-level Risk Assessment. These range from generic guidance which applies to Risk Analysis at the national level, to specific guidance looking at Critical Information Infrastructures (CII). Below we summarise five of the publicly available guidance and documents relating to the practice of risk analysis which the research team consider useful, as they are comprehensive and cover the issues from a methodological or programmatic perspective. Our review identified some useful guidance on the practice of risk assessment in the context of national and international risks, but much of the Critical Information Infrastructure risk analysis guidance identified concerns risk analysis in the context of organisational ICT risks, rather than national-level risk assessment. For example, although many internationally available standards such as ISO 27005: 2008[28], ISO 15408: 2009[29] and ISO 31010:2009[30] contain guidance on risk analysis they are often framed at the system or organisational rather than the national level. Of the five guidance documents summarised below two are aimed at national-level assessment and two at the organisational level.

The International Risk Governance Council (IRGC) published a report in 2006 setting out an integrated framework for how national-level risk analysis initiatives might be set up (International Risk Governance Council 2005). It provides guidance for the development of comprehensive assessment and management strategies to cope with risks. The framework is focused on those risks with international implications which have the potential to harm human health and safety, the economy, the environment and/or the fabric of society at large, but it is not on Information (cyber) Risk Management. The IRGC report is instructive for its breadth of analysis of terminology, its focus on the process of undertaking a national-level risk assessment, and the importance it places on understanding the context and environment in which a risk assessment is conducted.

The Institute for the Protection of the Security of the Citizen (IPSC), part of the Joint Research Centre (JRC) in Ispra, Italy, published a Technical Note containing a compendium of 19 different Risk Analysis methodologies applicable at the national level in the context of Critical Infrastructure Protection (CIP) (Giannopoulous et al. 2012). This finds that although there are a significant number of risk assessment methodologies each with a common and linear approach (identification and classification of threats, identification of vulnerabilities and evaluation of impact), there is a huge difference between methodologies in their scope, intended audience and domain of applicability. This report also finds that risk assessment methodologies can be further categorised by whether they are for a particular sector or whether they take a systems approach.

Some guidance was identified on conducting cyber-security and CII-related Risk Assessments at the organisational level. Examples include those from the US National Institute of Standards and

[28] ISO/IEC 27005:2008 Information technology -- Security techniques -- Information security risk management
[29] ISO/IEC 15408-1: 2009 Information Technology – Security Techniques – Evaluation Criteria for IT Security – Part 1: Introduction and General Model
[30] ISO/IEC 31010:2009 - Risk Management - Risk Assessment Techniques

Technology (NIST) and the UK HMG Technical Risk Assessment IA Standard No. 1. In addition, ENISA has an extensive inventory of the most common Risk Analysis methods. The catalogue isavailable on ENISA's website.[31]

In September 2012 NIST released a Guide for conducting Risk Assessments (NIST 2012). It notes that risk assessment is done throughout an organisation. It indicates that there are no formal requirements for a risk analysis, and organisations (by which is meant the US government) should have maximum flexibility in applying guidance. Importantly, the limitations of risk analysis are described, including that they are often not precise instruments of measurement, and that the outputs are of course dependent upon the quality of information provided, the limitations of specific methodologies, tools and techniques used and the subjectivity, trustworthiness and quality of the data, the interpretation of results, and the skills and capabilities of individuals or groups conducting the assessment.

The UK's Technical Risk Assessment IA Standard No. 1 (issue 3.51) from 2009 (CESG & Cabinet Office 2009) is a component of the UK government's policy framework and is intended to be used across the public sector. It provides a framework for identifying, assessing and determining the level of risk to an ICT system. This guidance is useful in including an understanding of the risk analysis lifecycle (how it fits into the process of applying measures to manage the risk), as well as containing a practical worked example.

The US National Academies of Science (NAS) evaluated the different risk analysis methods used in the US Department of Homeland Security (DHS) in a report published in 2010.[32] This found that although a generally appropriate conceptual framework had been developed, no capabilities and methods appeared adequate for supporting DHS decision-making with the exception of risk analysis for natural disasters. It made a number of recommendations including improvements to the way in which models are used following scientific practices, and building a strong culture of risk analysis.

3.2 National context for cyber security

In this section we summarise results from the fieldwork concerning the national context for cyber security. The national context is important as it informs the work and outputs of any national risk assessment programme. For example, without national-level policy ownership of these issues, the results of a National-level Risk Assessment might go unheeded.

In some of the countries studied, cyber National-level Risk Assessments sometimes sit alongside risk assessments done in other sectors. Figure 5 illustrates the national-level structures when this is the case.

[31] ENISA Inventory of Risk Management/ Risk Assessment Methods (2011) http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods

[32] Committee to Review the Department of Homeland Security's Approach to Risk Analysis (2012) National Research Council of the National Academies Review of the Department of Homeland Security's Approach to Risk Analysis Washington DC 2010

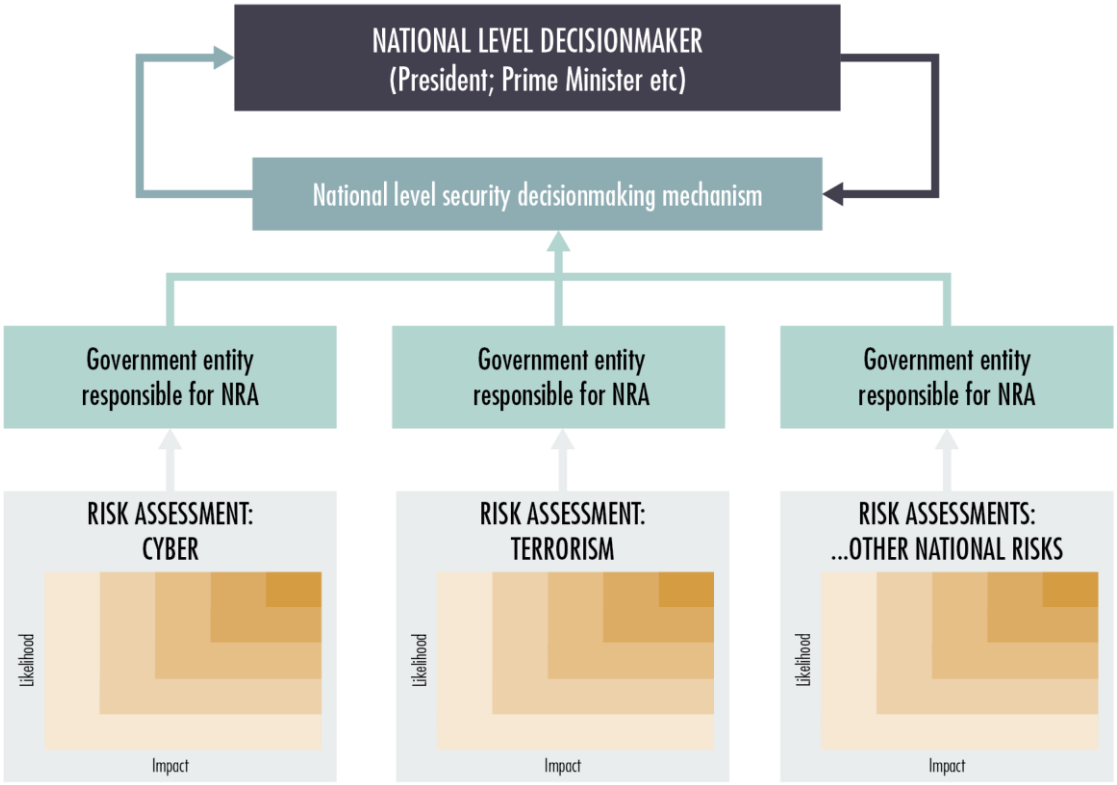


Figure 5: Risk inputs to senior decision-makers

3.2.1 Countries having a National Cyber Security Strategy

A National Cyber Security Strategy (NCSS) may be considered as a key background component of a National-level Risk Assessment. An NCSS should outline the role that the National-level Risk Assessment plays and how it might contribute to prevention of crises. ENISA maintains an online directory on NCSS across the world and undertook a study into NCSS in 2012 (ENISA 2013c).

Six countries consulted in the study have a specific NCSS (United Kingdom, Finland, Germany, Estonia, the Netherlands and Switzerland) in place. In Finland, this has been released most recently (January 2013) and is currently in its implementation phase. In Estonia, the strategy is being revised at the time of writing. In Spain, the national Cyber Security Strategy has been developed by representatives from the Ministry of the Interior, defence industry and the CNPIC (the National Centre for Critical Infrastructure Protection) but is pending approval. In some other countries there is no specific National Cyber Security Strategy, though in Sweden efforts are underway to develop one. For comparison, Japan's latest revision to its national Cyber Security Strategy was due in June 2013, having first been published in 2006.

3.2.2 Organisations with a mandate to address cyber security and /or CIIP

Next, we consider the presence of a designated cyber security organisation or authority in the countries consulted in the study. National-level organisations with a responsibility to consider cyber security are key stakeholders of a National-level Risk Assessment – either by conducting the National-level Risk Assessment themselves or by providing assurance on risk assessments conducted by other stakeholders (see below). Depending on the nature of the national-level organisation they

may also have responsibility for CIIP, or responsibility may lie within a separate agency or even a telecommunications regulator.

Across the countries on which information was collected, policy-level ownership of cyber security and CIIP was held in different types of organisation. Some had a designated cyber security agency (such as the Office of Cyber Security and Information Assurance (OCSIA) in the UK) whilst in others the interior ministry, telecommunications regulator or other entity was responsible at the national level for cyber security. Also, there are cases where cyber security responsibilities are shared among a number of public entities, with no single designated authority. Understanding how the policy ownership of cyber security works is important because the nature of the national-level body or bodies with ownership of cyber security will inform what particular risks are prioritised and how the risks need to be communicated for maximum impact.

In the UK the OCSIA works closely with lead departments and CCS to ensure that cyber security risks are effectively represented in the National Risk Register.

In Estonia, a specific Information Systems Authority (Riigi Infosüsteemi Amet – RIA) is responsible for covering cyber and information security. RIA is a sub-division of the Ministry of Economic Affairs and Communications and its focus is on protection of information systems necessary for the functioning of vital services. In Denmark, the national IT security authority resides in the Centre for Cyber Security. The Centre is responsible for providing a threat analysis.

In France, the ANSSI (Agence nationale de la sécurité des systèmes d'information) was created in 2009 to address IT systems security across a number of vital sectors and to help the private sector achieve security. ANSSI reports to the SGDSN (Secrétariate général de la défense et de la sécurité nationale), which then reports to the Prime Minister.

In Germany, the German Federal Office for Information Security (BSI) currently acts as the national security agency to promote IT security in the country. Alongside the Ministry of Interior and the UP-KRITIS[33] PPP it conducts detailed work on threat and risk analysis.

In the United States, the Department of Homeland Security (DHS) has the federal mandate to tackle the civilian aspects of CIIP under the vision set by the Executive Branch (the White House).

3.2.3 Other actors in cyber security collaboration

Actors in cyber security collaboration within the countries consulted in the study also include ministries and government departments. In most countries consulted Ministries of the Interior are responsible for civil protection, overall coordination and regulation of crises and emergencies and often play an important part in cyber security collaboration. They may undertake coordination of the national cyber security strategy or they may host centres to protect critical infrastructure, such as the National Centre for Critical Infrastructure Protection in Spain. Ministries of Justice may also be involved: for example, the Dutch National Cyber Security Centre (NCSC) is part of the Ministry of Safety and Justice and of the National Coordinator for Counterterrorism and Security (NCTV). In Germany, a role is also played by the Federal Ministry of Economics and Technology and in the UK by the Department of Business, Innovation and Skills (BIS). In South Korea, the National Intelligence Service and the Ministry of Science, ICT and Future Planning are officially responsible for cyber security.

[33] Bundesministerium des Innern (2007) CIP Implementation Plan of the National Plan for Information Infrastructure Protection ('UP-KRITIS') As of 13 October 2013: http://www.bmi.bund.de/SharedDocs/Downloads/EN/Broschueren/2009/kritis.html

3.2.4 Examples of coordination among different actors in the cyber security arena

As cyber security is a cross-domain issue, in order to derive an accurate appreciation of the risks, input must be taken from a range of entities in the public and private sector.

Most countries are aware of the importance of coordination with public and private sector actors, even if they might not necessarily have a centralised national coordination authority. In Spain, for example, the National Centre for Critical Infrastructure Protection (CNPIC) located within the Spanish Ministry of the Interior is tasked with conducting RAs to evaluate physical and cyber threats and works closely with public and private sectors (e.g. critical infrastructure managers). CNPIC also communicates with the National Antiterrorism Coordination Centre, which provides CNPIC with risk analyses that are then integrated into its assessments.

In the UK, the Department of Business, Innovation and Skills (BIS) is responsible for a significant part of the cyber security strategy, especially with regard to issues concerning the private sector. The Office of Cyber Security & Information Assurance (OCSIA) works in close cooperation with Government Communications Headquarters (GCHQ) and receives and analyses intelligence from public sector agencies, allowing them to identify and prioritise threats.

In some countries the coordination function is performed by a specific cyber security centre. In Japan, coordination between actors in cyber security is provided by the National Information Security Center (NISC) which acts as a facilitator of information security efforts of government agencies and a point of contact for international affairs. NISC coordinates Critical Infrastructure sector-specific ministries, related organisations and designated sectors including, for example, information and communications, finance, aviation, railways, etc. The ISPC (Information Security Policy Council) is a supreme body for endorsing important cyber security policies. Similarly, the National Cyber Security Centre (NCSC) in the Netherlands performs a coordinating function between government departments and between private and public sectors in a relatively decentralised system where government departments and different private sector actors are responsible for different aspects of cyber security.

In the United States, the Department for Homeland Security's Office of Cyber Security and Communications plays a role in regard to non-military critical infrastructure within US federal efforts. This is under the auspices of the 2009 National Infrastructure Protection Plan (NIPP) and the Executive Order from the White House of February 2013 (White House 2013). These are fed into the US National Security Committee as the highest-level organisation responsible for analysing all national-level risks to the United States. Within DHS, the Homeland Infrastructure Threat and Risk Analysis Centre (HITRAC) performs risk analyses for the 16 critical infrastructures. DHS units link, via a range of other mechanisms such as the Partnership for Critical Infrastructure Security (PCIS), sector coordinating councils and Information Sharing and Analysis centres, to pull together a Risk Profile for each Sector under the Critical Infrastructure Partnership Advisory Council CIPAC).

Some countries have set up a specific high-level cyber security council – a political body, including members from different ministries. In Germany, the council receives some input from the PPP set up in the country to share insights from practitioners' perspectives. In Estonia, the Cyber Security Council is a sub-council of the general-level Security Council and is responsible for approving cyber security strategy. The Critical Information Infrastructure Protection (CIIP) Council which includes representatives from both public and private sector reports to the Cyber Security Council. Both councils meet regularly.

Coordinating efforts across different sectors have also been in place in Finland, where the national cyber security strategy was coordinated by the Security Committee chaired by a senior civil servant and including representatives from government ministries.

3.2.5 The decentralised National-level Risk Assessment approach

Some countries have adopted decentralised approaches. In summary this approach is a different way to undertake National-level Risk Assessment since it relies upon each actor completing their part of the Risk Assessment in a decentralised fashion. Figure 6 outlines the differences between the decentralised and centralised National-level Risk Assessment approach.

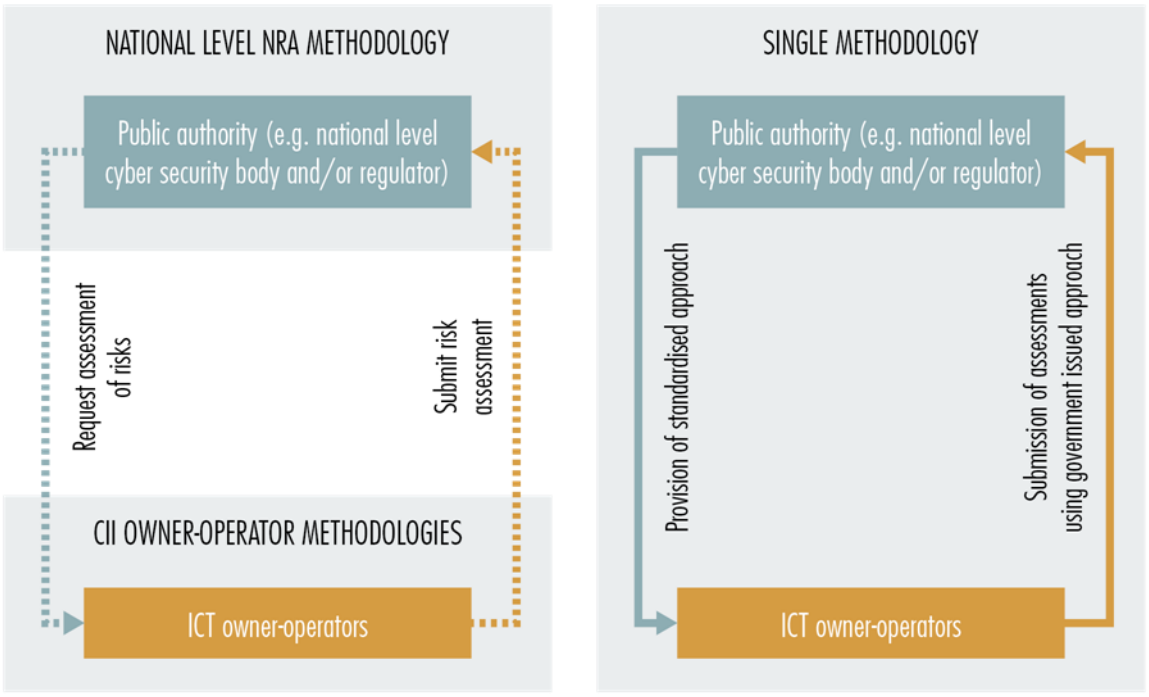


Figure 6: Decentralised and single methodology approach

The outcomes of these assessments then feed into the National-level Risk Assessment. A key aspect is maximising consistency across the different assessments, as they may have been produced using diverse methodologies.

Decentralised approaches are taken in Finland, Switzerland and Sweden, although information sharing and close relationships between public and private sector shareholders are recognised as important for risk analysis. In Finland, the practice of RA is devolved according to individual organisations. There is no single set of 'RA tools' which are applied at the organisational level, nor a 'normative' framework for risk analysis. In Switzerland, cyber risk is seen as an integral part of a wider overall risk picture. Notable cooperation took place during the preparation of the National strategy for Switzerland's protection against cyber risks. On an operational level, MELANI (the Reporting and Analysis Centre for Information Assurance), a coordination and reporting centre for incidents, plays a key role.

In Sweden, the lead agency for RA is the Swedish Civil Contingencies Agency (MSB) which provides nonbinding guidance and tools for others in a range of sectors to follow. PTS (the Swedish Post and Telecom Authority), which regulates the post and telecommunications sector, performs RAs annually in the area of CIIP using tools from the MSB. For counties and municipalities, a similarly decentralised approach is taken with delegated authorities for crisis management activities and RA.

There is a certain element of decentralisation also evident in the US approach, as each of the 16 critical infrastructures has its own sectoral body responsible for production of a risk assessment, which may be driven by different requirements – e.g. if a sector is highly regulated then the subsequent RA will be take on a similar character, perhaps being focused on issues of specific interest to the regulator. Each RA is reported to be analysed and quantified in terms meaningful to that particular sector.

3.2.6 Conclusions regarding the national context for cyber security

Among the 20 countries consulted as part of this study there are considerable differences concerning which public administration has the policy responsibility (or is the 'customer') for risk assessments undertaken in the domain of CII. Therefore, this is likely to have an impact upon how the risk analysis is performed (what particular priorities are accorded to different aspects within it) and the approach used to communicate the results of any National-level Risk Assessment to senior decision-makers.

3.3 Overview of findings relating to National-level Risk Assessment programmes

In this section we present the main findings from the research as they relate specifically to National-level Risk Assessment in this domain. We identify commonalities and variations in the approaches for threat assessment, how countries have implemented their National-level Risk Assessment, key challenges and lessons learned. Table 1 summarises all these, while Figure 7 illustrates the possible inputs to the National-level Risk Assessment.

Aspect of implementation	Variations / examples
Approaches to a National-level Risk Assessment are either:	Through a formalised RA By decentralised RAs
National-level methodologies can be based on:	Scenario-based approaches Qualitative or quantitative approaches Combined approaches

Table 1: Summary of findings

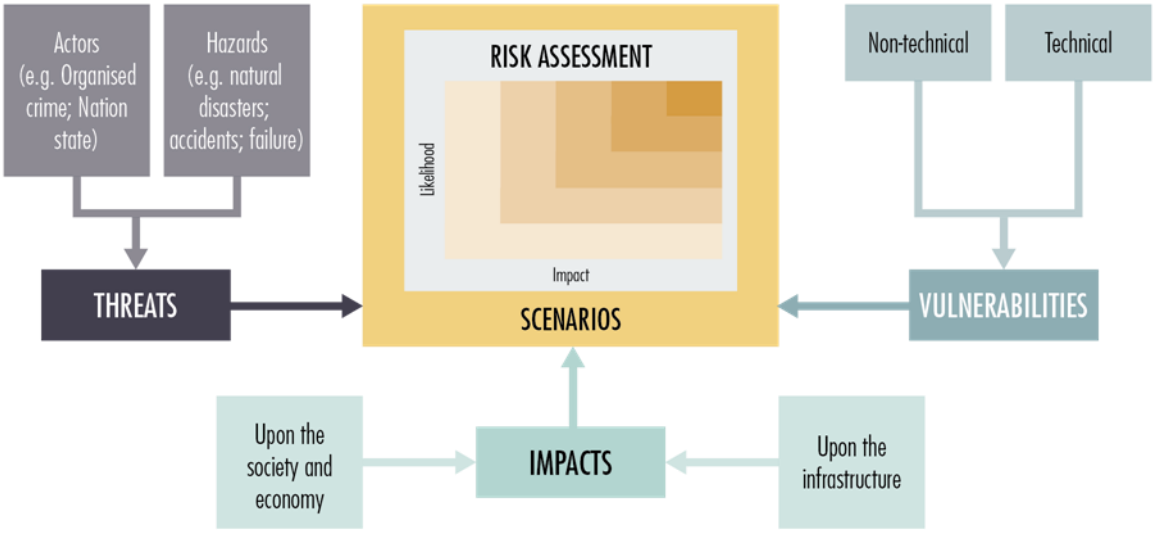
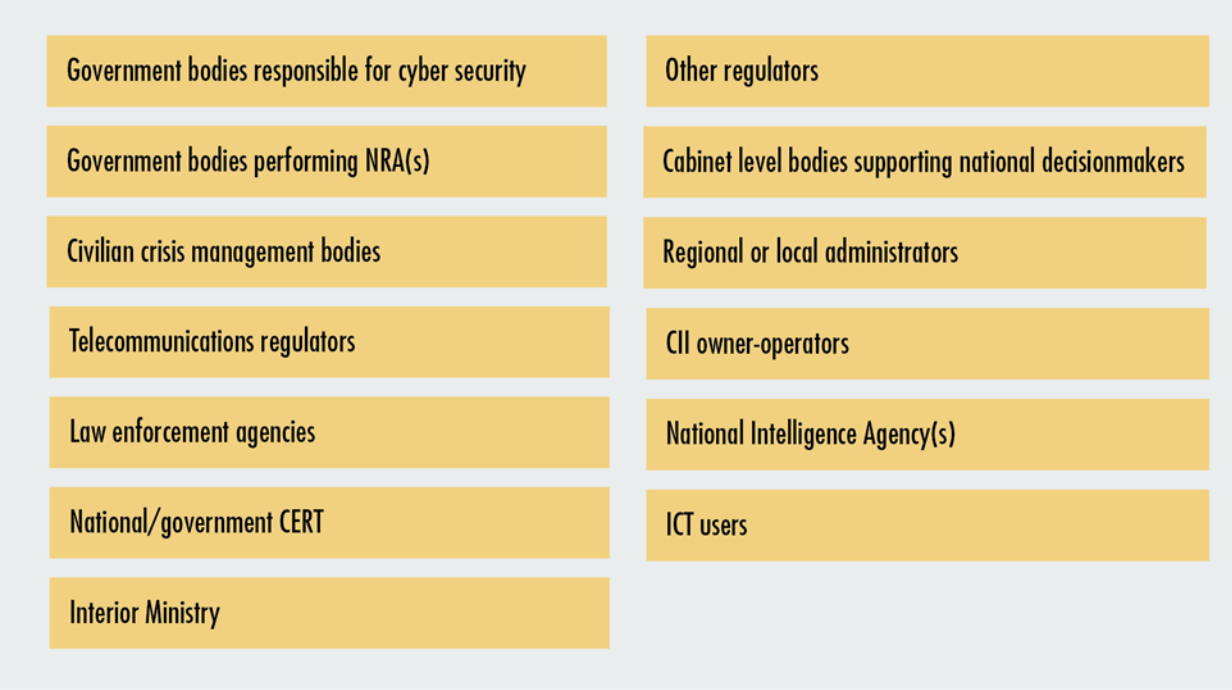


Figure 7: Possible inputs to the National-level Risk Assessment

Figure 8 illustrates the diversity of organisations reported in this study as having some kind of involvement in National-level Risk Assessments. Which of these organisations might be involved is sometimes quite dependent upon the national context. Other aproaches on this process have been described by ENISA in its previous work on risk management[34].



[34] Risk Management process, http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-process

Figure 8: Organisations analysed as having some kind of role in conducting National-level Risk Assessments

3.4 Approaches to threat modelling

In this section we will look at the different aspects of the threat modelling and characterisation, including the terminology and approaches used.

3.4.1 Terminology in threat modelling

Definitions of specific terms differ across countries and sometimes also within countries. The majority of countries under review have adopted their own definitions of key terms such as 'threat', 'vital services'; 'strategic sectors', 'national security interests'; 'risk' and 'critical risk'. However, categorisation of threats may differ both between EU countries and between different sectors within a country. Some countries have specific threat catalogues in place, though this does not automatically mean they have a standard definition of what a threat is. Security objectives are in some cases outlined in very generic terms. There is no single international categorisation on threat criticality. In addition, for some countries threat assessment can be very sensitive.

3.4.2 Threats addressed in national security strategies

Cyber threats can be addressed in specific cyber security strategies or in more general national security strategies. In the UK, the National Security Strategy (NSS) addresses threats and trends relating to domestic and international security. This is informed by the National-level Risk Assessment, which deals with accidental and deliberate types of risk (including cyber). Within the strategy, 'national security interests' are defined broadly as 'secure spaces within the UK', encompassing protection of UK well-being, infrastructure, way of life, etc. Cyber is identified as 'priority one' risk, with other priority one risks including terrorism and state threats.

In Finland, a number of threat characterisations are included in the 2010 Strategy for Society Security. These can be used to inform new regulations. The 2010 strategy does not identify any specific 'adversaries', but the 2013 Cyber Security Strategy identifies a range of threats including 'hacktivism'; 'cyber-criminality'; 'cyber-terrorism' and 'cyber-espionage'.

The Swiss Cyber Strategy sets out definitions of terminology (e.g. 'risk' and 'critical risk'). MELANI[35] applies 'thresholds' when classifying risks by their probability but it tries to avoid thresholds where possible due to the complexity of the risks. With regard to cyber risks, there is an emphasis on qualitative assessments as quantitative assessments often relate to vulnerability, yet it is argued that actual threat is more important than vulnerability in the cyber domain.

3.4.3 Scenario-based approaches

Several countries use scenario-based approaches to assess threats.

In Estonia, the importance of threats is determined based on two dimensions: (1) threats to a defined list of vital services and (2) the Emergencies Act which describes an emergency situation. One such emergency is defined as 'a large scale cyber-attack' and there is a response plan for this scenario. With the help of public and private sector discussion, scenarios were formulated together with response plans to different cyber attack scenarios.

[35] MELANI – Reporting and Analysis Centre for Information Assurance http://www.melani.admin.ch/?lang=en

In Germany, the Ministry of the Interior takes responsibility for threat assessments. For general threats to critical infrastructure, a Public–Private Partnership (PPP) was set up under the UP-KRITIS programme concerned with the operation of critical infrastructures such as transport, food, energy, ICT, health, etc. To share problems/ threats from the practitioners' perspective, this PPP inputs information to the Ministry of the Interior. The PPP uses a scenario-based approach in which the group considers potential responses to a threat scenario analysed on different levels. One of the challenges is the complexity of finding an objective route to weigh/determine formal measures of probability. Initiatives focus on the most important processes/services that should not be interrupted, such as the financial sector or ICT.

3.4.4 Quantitative approaches

Unlike many EU countries, risk assessment in Japan is quantitative in nature. Risk Analysis is conducted by a CIP Committee under the Information Security Policy Council (ISPC). The threat model is structured around four kinds of threats. These are defined in the Second Action Plan for Information Security of Critical Infrastructure and include: (1) Intentional factors (e.g. cyber attack); (2) Non-intentional factors; (3) Disaster (i.e. external factors); (4) Impact from other sectors (e.g. blackouts). The relevance of these four categories is evaluated annually. The model does not cover detailed 'sub-categorisation' within these threat types. The model is used on two levels: (1) a service level and (2) a verification level.

3.4.5 Qualitative approaches

Countries with a specific threat modelling technique in place tend to use qualitative models. Qualitative assessments (although quantitative assessments of vulnerability are often made) are the usual approach used by countries when deciding upon the significance of a threat. Qualitative models with a broad range of threats are common in the Nordic countries and the Netherlands. Some countries use the geographical scope of the consequences (e.g. local, regional, national approach) to determine how critical a threat is.

In the Netherlands, different methodologies are used to characterise threats in different sectors and departments. The NCSC threat model used during an annual cyber security risk assessment includes state and non-state actors (terrorists, hacktivists, script kiddies, etc.). Threats are ranked using a high-medium-low scoring system based on a qualitative assessment.

France places threats into three categories: espionage, destructive attacks and attacks on integrity.

In Denmark, the Danish Emergency Management Agency acts as a coordinating committee and considers a broad spectrum of threats at the national level. The Agency focuses on consequences and preparedness. The Danish model divides threats into: 'nation state actors' and 'non-nation state actors'. Faced with the latter (e.g. cyber-criminals), the Centre for Cyber Security manages emergency recovery while the police are responsible for prosecutions.

Sweden uses an 'all-hazards' approach. The model looks at a wide range of threats which include unauthorised use of information, eavesdropping and technical malfunctions of systems, intended or unintended. Validation of threats takes place at the level of the Swedish Civil Contingency Board. It might be so that a validation also, on a sub-level, could takes place within an sector. Risks are linked to the five national values of protection established by the Swedish government. This analysis also considers vulnerabilities and consequences.

3.4.6 Threat modelling under development

Some countries have not yet fully deployed a threat modelling methodology. For example, the Spanish CNPIC has so far defined twelve strategic sectors and is currently developing a plan to

address sector-specific threats. This plan will use a top-down methodology. CNPIC is collaborating with ministries with sector-specific expertise (e.g. the Ministry of Industry) in order to identify sector-specific threats. Once the plan is finalised, CNPIC will work with infrastructure operators.

3.4.7 Conclusions for threat modelling

Most of the countries that participated in this research used a *qualitative* understanding of the threats, although there was an intricate quantitative model identified. Many countries split the threat actor/agent from the attack means/vector.

It should be stressed that more work is needed in the area of cyber threat modelling; current approaches are developed in an ad-hoc manner and insular. Currently, there is no clear standard or practices in place. This may be a direct result of the very fast-changing threat landscape, as highlighted by ENISA's reports (see ENISA 2013b).

3.5 Approaches to Risk Assessment

In this section we summarise what risk analysis methodologies have been deployed by the participants in the research. In some cases we gained detailed information on specific methodologies deployed.

3.5.1 RA strategy

Some of the countries analysed have a formalised National-level Risk Assessment framework in place. As an example, in the UK the National-level Risk Assessment informs responses to security threats. The National-level Risk Assessment is approved by both ministers and chief scientists. The success of the National-level Risk Assessment in the UK model depends on the 'buy-in' of a range of government departments. The National-level Risk Assessment does not focus on private sector issues such as companies' vulnerability. Management of specific risks, in turn, is owned by the department or agency with relevant expertise in that area. When a department 'owns' a risk, it is responsible for reviewing and updating it in the National-level Risk Assessment on an annual basis, as well as for risk mitigation. Where risk ownership is unclear, the Cabinet Office is the default owner. The NCSS addresses impact on business, national security threats, awareness, cybercrime, etc. Figure 9 outlines how these mechanisms work between different organisations.

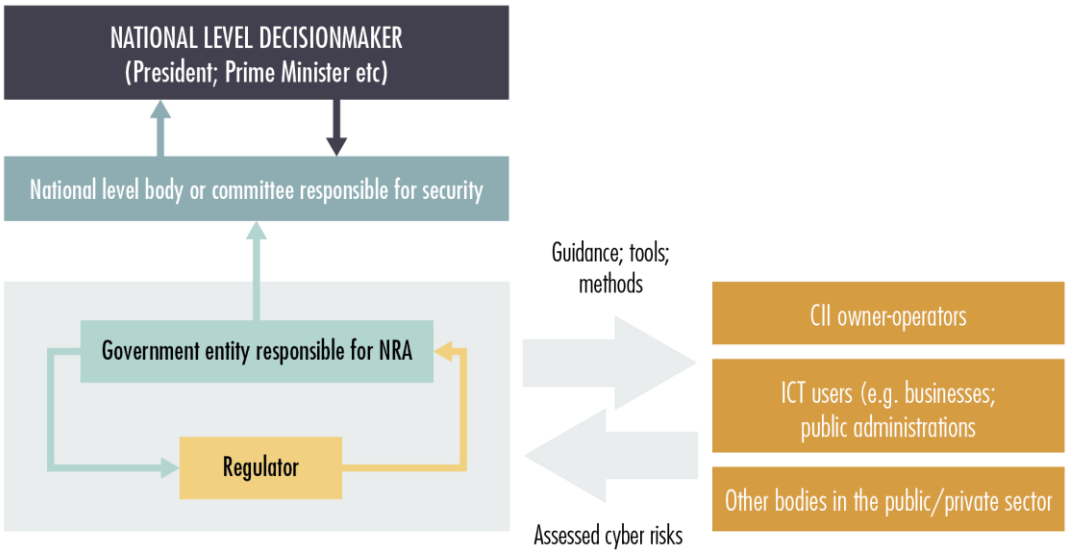


Figure 9: Interactions between public and private sector in the NRA process

In Estonia, the Ministry of the Interior prepares a single restricted document based on RA carried out by critical services every year. This RA is sent off to relevant ministries and agencies which synthesise the results. Different ministries and public sector agencies play a crucial role in reviewing the statements of different vital service providers to ensure correct reporting. Specific glossaries are used to ensure consistent usage of terminology.

3.5.2 Decentralised RA

The Nordic countries and Switzerland have a more decentralised RA devolved to individual organisations. There is no single set of 'RA tools' to apply at the organisational level, or a 'normative' framework for RA. Cyber risk may be seen as a part of a wider overall risk picture.

In Sweden, the lead agency in RA is the Swedish Civil Contingencies Agency (MSB) which provides mandates for other sectoral organisations. Sweden has a decentralised approach whereby sectors are responsible for drawing up an RA. In Denmark, RA is the responsibility of each telecommunications company as a national-level RA is deemed unviable. It is worth noting that a similar situation exists in Japan, where telecommunications operators and industries use different RA models with a range of terms and definitions. There is no unified RA model as separate sectors face distinct types of risk. RA takes place every 1–2 years as part of a Plan, Do, Check, Act (PDCA) cycle.

3.5.3 Conclusions for approaches to Risk Assessment

There are a variety of approaches taken to RA on a spectrum of centralised to decentralised models. This may be driven by prevailing contextual factors in a particular country; for instance, the extent to which other stakeholders can be required to follow a particular standard for National-level Risk Assessments or whether this could be successfully accomplished using 'softer' policy mechanisms.

Further research is required to assess which of the approaches best fit specific national-level risk mitigation strategies. National-level cyber risk assessment is still an emergent activity which will require a number of iterations in order to truly define best practices. Initiatives such as this study, by providing an overview of existing approaches, could well lead to better risk assessments in the future.

3.6 National-level RA methodologies in use

RA methodology differs from country to country, with some countries consulted in the study not using a formalised methodology. Figure 10 illustrates the main differences between the various methodologies reported in use.

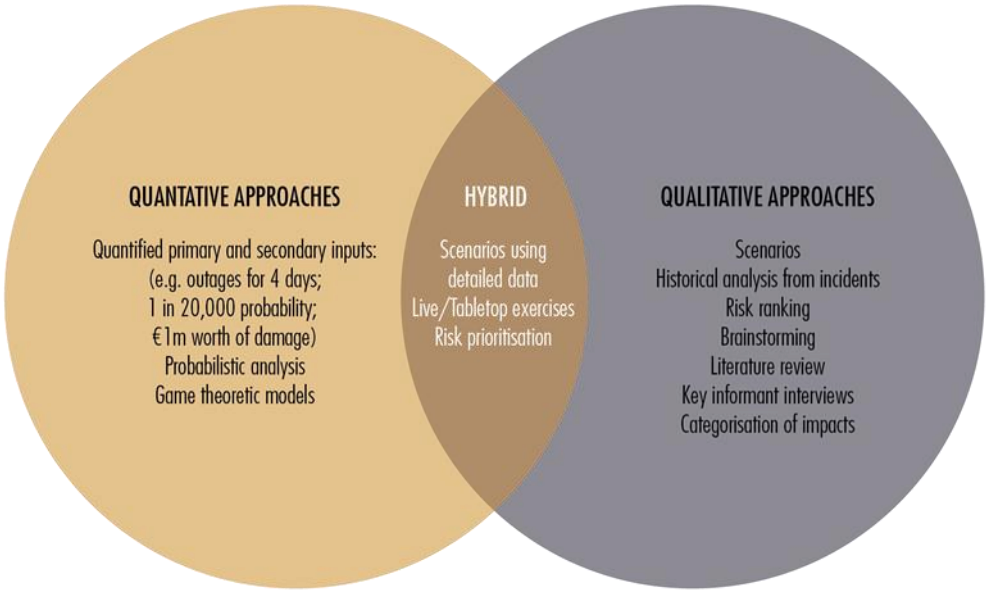


Figure 10: Examples of quantitative, hybrid and qualitative approaches

3.6.1 Scenario-based approach

A scenario-based approach is an RA methodology used by some countries in our research. In the UK, RA is undertaken as part of a three-stage process based on a scenario-focused approach: (1) departments and agencies provide information on scenarios; (2) a cross-government discussion follows to determine whether these are the appropriate scenarios to be considered (this consultation involves chief scientists and policy/ economics/ intelligence experts) and (3) scenarios are finally assessed according to impact and plausibility.

Measuring impact and plausibility: case of the UK Impact is measured in terms of casualties, fatalities, economic harm (reduced GDP), social disruption and psychological impact. Measuring impact involves the risk owner and other government departments with relevant expertise and/or likely to be most affected by the scenario. Plausibility is determined by intelligence from other

government authorities. This criterion uses a logarithmic scale to determine the order of magnitude ranging from 1 in 2 to a 1 in 20,000 likelihood.

The private sector facing element of the RA is carried out by the Centre for Protection of National Infrastructure (CPNI), which operates on a more asset-based model, identifying critical assets Adapting this to the cyber context might be challenging as it requires a more systems-based, rather than asset-based approach (due to the complex interdependencies in cyberspace). Lastly, the Civil Contingencies Secretariat (CCS) concentrates on supporting government efforts around RA, preparation and planning, response and recovery, and resilience.

In the telecommunications sector, Denmark also uses a scenario-based approach. The RA for this sector includes probabilistic events (accidents, natural catastrophes, etc.) in a handful of online scenarios. Within each scenario, guidance is provided on how to act in each situation but there is no explanation for the primary reasons why an attack may occur.

In the US, in the civilian domain, the HITRAC program and the Risk and Modelling and Simulation Unit in the DHS provide a risk estimate which is expressed in qualitative risk pairs (a list of each risk with its consequence and likelihood). These risk pairs cover an all-hazards approach (including accidents and natural disasters) and cover both physical and cyber-related risks.

Qualitative and quantitative tools in Sweden. In Sweden, a combination of qualitative and quantitative tools are used to assess risks related to particular scenarios with regard to consequences and the likelihood of a similar event occurring in Sweden. Scenarios are developed according to criteria that include over 20 context-forming variables such as location, time and area of impact. Impact of the threat is then categorised (if possible) according to the geographic scope of the consequences (local, regional, national) and the duration of the disruption. These details are then used to estimate the overall impact on the sector. Additionally, societal consequences are assessed according to a 5-grade scale. These are expressed in qualitative terms. The Swedish national risk assessment also covers antagonistic threats. Disruptions to electronic communications have been identified as one of 27 particularly serious (national) events that are gradually being subjected to more in-depth analysis.

3.6.2 Combination of different approaches

Some countries combine different approaches in their RA methodology, often inspired by methodologies used in different countries and based on standards adopted internationally. In Estonia, the RA methodology is based on guidelines from the Ministry of the Interior which are in turn based on different methodologies and various international standards adapted to the Estonian case; for example BS 25999 (now ISO 22301),[36] ISKE[37] and the German BSI standards.[38] Five levels of probability measures are defined and used in the RA guide.

In Switzerland, the Swiss Office of Civil Protection has designed a toolkit to go alongside the National Strategy for Switzerland's protection against cyber risks. It takes known ISO methodologies and combines them with those in the German handbook for critical infrastructure. The toolkit does not

[36] ISO, 'ISO 22301: 2012', Standards catalogue. As of 22 August 2013: http://www.iso.org/iso/catalogue_detail?csnumber=50038

[37] Estonian Information System's Authority, 'Three-level IT baseline security system ISKE', 10 May 2012. As of 22 August 2013: https://www.ria.ee/iske-en

[38] Federal Office for Information Security (BSI), website. As of 22 August 2013: https://www.bsi.bund.de/EN/TheBSI/thebsi_node.html

focus merely on cyber security, but integrates it with physical and personnel security. The MELANI approach uses sector-specific standards for RA, depending on the scenario.

The new RA framework in France is based on a well-established organisational level RA approach known as EBIOS (ANSSI 2010) focused on physical security that looks at the sector, seeks to identify threats and design how best address them. Cyber is integrated in all the different models/ sectors (a specified number of sectors and sub-sectors including energy, transport and defence). Each sector evaluates risks at three levels: macro, mid and micro. A qualitative approach is taken to determine the most important risks. Precise probabilities are not used. The same methodology is used for every type of RA at both the micro and macro levels. The importance of updating risk assessments to ensure they stay relevant is recognised in this context.

3.6.3 Other approaches and work in progress

In some cases, there is a perception that a national RA methodology is less of a priority than dealing with pan-European problems (e.g. pan-European computer incidents). Despite the lack of a national risk framework for cyber, significant technical work carried out by CERTs may still prove useful, as in the case of Portugal.

In another country we studied, the RA is based on the predicted impact on different processes in the critical sectors. During discussions on RA within the multi-stakeholder discussion group, however, neither 'risk', nor 'impact' were said to be clearly defined in this country. RA practitioners used interviews, brainstorming and discussion to determine threats. They focused on listening to industry advisors' recommendations as the best way to gain an accurate sense of the risk landscape. In this particular country, operators are expected to assess their own risks.

In many countries the development of an RA methodology may be considered a work in progress. The Spanish CNPIC is working on a three-point impact assessment to evaluate:

(1) impact on personnel (casualties);
(2) impact on national economy;
(3) environmental impact;
(4) impact on the society wellbeing.

The Centre has identified five thresholds which are classified and measured quantitatively. CNPIC personnel are currently taught to use 'Magerit', a risk assessment methodology used predominantly in the public sector, publicly available in Spanish.[39] This methodology is primarily used to assess probability.

3.6.4 Conclusions for methodologies used

There are a variety of methodologies deployed for RA, including those using qualitative and quantitative methods. Some countries have adopted a hybrid approach whilst other countries are at an emergent stage with respect to the choice of a particular methodology.

3.7 Key challenges from national experiences

Interviewees and questionnaire respondents were asked to identify what they perceived to be the key challenges facing their country in relation to national-level RA for cyber security. The following were the most commonly mentioned: (1) lack of harmonised legal framework; (2) incomplete and

[39] Ministerio de Administraciones Publicas (Spanish Ministry for Public Administrations) (2005) Magerit v.2 As of 13 October 2013: http://www.csi.map.es/csi/pg5m20.htm

diverse risk assessment methodologies; (3) getting a comprehensive understanding of threats; (4) effective risk management and preparedness; (5) insufficient information sharing. Below we describe the nature of the problem as characterised by those participating in the research.

3.7.1 Lack of harmonised legal framework for cyber security

This barrier to a more effective cyber security system takes various forms. Most commonly, countries have adopted different definitions, or only vague definitions of key terms such as 'critical information infrastructure', 'risk', 'threat', or 'priority risks', etc., which can hinder an effective harmonisation of risk assessment. Risk assessment is often decentralised and different RA tools are provided by different (sometimes private) providers. With no harmonised legal framework, it is difficult to talk about minimum standards. Moreover, opinions differ among countries as to the usefulness of a minimum standards requirement or minimum level of maturity to implement National-level Risk Assessment.

3.7.2 Incomplete and diverse risk assessment methodologies

The diversity of methods used in RA process by different countries was reported by participants to pose a serious challenge to a coherent pan-European cyber security approach. In some countries, different sectors have their own priorities and there is no unified method to prioritise risk; others use an 'all-hazards' approach. Some participants argue that an all-hazards approach might not be the most effective as it covers a wide range of different types of risks which are very diverse and could, potentially, be better dealt with in clusters. However, 'clustering' presents its own challenges as it raises questions about how to group/model actors' intentionality of threat. Additionally, participants mentioned methodological challenges in measuring the value of assets, economic costs, providing gross assessments of likelihood of threat for scenario-based RA and prioritising systems that need protection. RA methodology should be continually reviewed and updated to include new information on new threats. Reconciling different risk assessment practices and standards across companies may also be difficult.

France and EBIOS. It was reported that France is currently reviewing its EBIOS methodology (which is consistent with the ISO27005:2008 Information Technology – Security Techniques – Information Security Risk Management) Specification for an Information Security Management System) to make it more suitable for use at a national level. This is an example of how methodologies might be revisited as countries get more sophisticated in their National-level Risk Assessment programmes.

3.7.3 Lack of comprehensive methods to assess threats

A key challenge reported by respondents is assessing threats and how they affect public/private sectors and society. A better understanding of threats leads to a better understanding of risk. Identifying cyber risks has been highly challenging due to both the large scope of threats and risks and the immediacy of current threats, which lead cyber security actors to favour a more reactive approach. But such a reactive approach may have partly prevented development of a more comprehensive threat model. To enhance countries' understanding of threats, it was suggested that a common taxonomy of threats in the electronic communications sector shared by all countries in the EU could be developed. As part of the RA, some mechanism to determine likelihood could be developed for threat actors, particularly those with hostile intent.

3.7.4 Need for effective risk management and preparedness capacity and skills

Participants reported that consultation on cyber security and CII risks often involves working through a scientific advisory committee to address best sources of evidence and to build in an independent scientific review base. In terms of risk preparedness, this differs between organisations, and often

depends on the amount of RA training they have received – particularly among vital service providers. For a sustainable level of preparedness, staff should be trained and competent to carry out the RA. Skilled and competent staff may, however, be difficult to find for every operator.

3.7.5 Information sharing

Various forms of information sharing have been proposed and tried in different countries, though many carry with them significant challenges.[40] Furthermore, opportunities to learn lessons from other countries are reportedly often hampered by budget limitations and difficulties in obtaining cyber information from operators. A key challenge identified by participants is how to coordinate the different perspectives of sectors and organisations and ensure better information sharing. One country reported the use of careful vetting and cooperative agreements to permit information to be pushed from government to the private sector.

3.7.6 Conclusions on key challenges from national experiences

The lack of a harmonised framework for cyber security could be considered as a key challenge (especially with regard to terminology) in addition to the diversity and relative uncertainties of current methodologies. Other key challenges were of a more systematic nature that affect many aspects of cyber security, including information sharing.

3.8 Lessons identified by respondents

3.8.1 Assimilating best practices and learning from international cooperation

One of the main lessons which respondents from several countries reported that they had learnt was recognising how useful international cooperation can be and how countries can learn from one another. Respondents from several countries recommended looking at good examples in Nordic countries which have experience in dealing with natural disasters, have published risk confidence indicators and have developed exercises that bridge intentions and actions. Some countries have also experienced fruitful cooperation with the US and Canada. Visiting centres in countries with relatively advanced CI capabilities such as the UK, Germany, US, Canada, France, Japan and the Netherlands has provided some countries with valuable best practice experience as they set up their own National-level Risk Assessment capabilities.

Several respondents expressed a preference for learning best practices from each other rather than imposing a single methodology at the EU level. The UK, for example, has recognised the importance of engaging with international stakeholders within the EU and OECD networks. The UK reported that this involved sharing best practice in identifying and assessing risk, for example through organising a summer 2013 conference among nations with relatively mature RA programmes to share experience; liaising with insurance companies and drawing on their advanced RA methods and using OECD research for examples of effective and ineffective approaches across a range of countries.

It was reported that the national RA in Sweden was inspired by a review of national risk assessments undertaken by the UK, Norway, the Netherlands and Canada. There is also an ongoing exchange of experiences from national risk assessments with other countries, the effectiveness of which was reported to be improving.

[40] Creation of PPPs in cyber security, for example, can be problematic as detailed information sharing in this context may be difficult due to the sensitivity and difficulty of obtaining information.

The respondent from one large EU Member State reported using best practice from other countries in a number of ways and considered this to be a very good way to support cyber security. More specifically, the use of ENISA good practice guides (e.g. the NSIE guide) and some guides from other Member States were highlighted by this respondent.

In terms of knowledge exchange once a programme is underway, the French ANSSI works with other international programmes and shares methodologies with them through systematic international collaborative platforms.

3.8.2 Relationships with the public and private sector

An effective cyber security system requires effective relationships among private and public sector actors. These can be nurtured through, for example, meetings with vital service providers as problems arise and particularly through good information sharing. A collaborative approach is deemed crucial to drive progress. For example, for the French ANSSI, it was reported that one of the main lessons learned was that a PPP is needed in addition to formal policy-making in order to build a strong relationship with the private sector. In the US, a key aspect noted to demonstrate to the private sector the business case of good cyber security practices concerned replacement of legacy equipment used in critical infrastructures. Conducting a National-level Risk Assessment was articulated as beneficial because of the fact that technologies likely to replace legacy equipment would be more reliant upon networks such as the public Internet.

3.8.3 Context-specific emergency responses and CI protection approaches

A frequently learnt lesson among the studied countries was reported to be that effective emergency responses and CI protection approaches have to be context-specific and that attempting to replicate other countries' approaches completely is not useful. Countries have important differences in legislation, culture and societal structure which have to be considered for any new initiative such as a National-level Risk Assessment programme to work well.

3.8.4 Conclusions on lessons learnt

Many countries are seeking to draw lessons from others in establishing or deploying a National-level Risk Assessment programme. The role of international platforms such as ENISA and the OECD would appear to be helpful in this regard, especially if the work done complements each other. As with many other cyber security issues, establishing good cooperation with the private sector and making sure that responses take account of contexts were also seen as important lessons identified, if not learnt.

3.9 Suggestions from Member States for National-level Risk Assessment development

In this final section we report findings about how countries participating in this research are considering onward development of National-level Risk Assessment efforts. An analysis of interview and questionnaire responses indicates that countries have recognised the following to be the key areas to address in the development of a National-level Risk Assessment: (1) greater understanding of threats and their effects on society; (2) better management of incidents; (3) greater stakeholder involvement and information sharing; (4) improved national CIIP frameworks and (5) guidelines on the EU level.

3.9.1 Greater understanding of threats and their effects on society

Most countries would like to focus on developing a better understanding of threats and how they affect public and private sectors and society more broadly. In practice at the national level, this would involve, for example, developing a good threat assessment mechanism that pulls together both threats and risks, creation of a cyber security centre to collect and share information on information security breaches, making risk analysis available to every system with a critical mission and focusing on understanding the rationale behind attacks.

3.9.2 Better management of incidents

Together with improving their understanding of threats, countries also recognise the need to improve the management of incidents. It was suggested that within the next 12–18 months there ought to be a robust understanding of risk and mitigation priorities. A specific suggestion from one respondent involved handling 'rare events' by developing a 20-year horizon scanning exercise that would resemble national risk assessment but could give a sense of alternative future scenarios.

3.9.3 Greater stakeholder involvement and information sharing

In the short to medium term, some EU countries expressed a desire to see involvement of more stakeholders such as SMEs in the process of RA and improving the cross-sectoral dialogue through PPPs. Most emphasised they would like to focus on bringing entities together particularly to share information on effective mitigation strategies. Another participant mentioned that the conduct of sector-specific table-top or regional exercises should be seen as a priority in order to help broaden the number of stakeholders.

3.9.4 Improved national CIIP frameworks

Several countries have specific steps in mind to improve their national CIIP frameworks. For example, one seeks to establish a framework that ensures that problems faced by operators (such as governance and systems management) are addressed effectively and operators are able to connect with their management to raise visibility of risks. This framework should also improve impact mapping. Others aim to develop a new RA model which would be more qualitative and would better consider sector interdependencies or seek to implement a strategy that will provide more resources to existing structures and ensure that government bodies understand and implement their mandates in the cyber area. There are other examples that want to combine legislation in an information society code, and others would like to focus more on including cross-border dimensions in their RA. One country in particular noted the difficulty of translating RA guidance and capacity building tools (e.g. self-assessments & training) from the organisational level to sector and then to national level.

3.9.5 EU guidelines and support

Several countries would like to see ENISA establishing a list of the most important cyber risk scenarios. They would also like to see the establishment of an international protocol for sharing information on best practices for National-level Risk Assessments, as suggested by one large EU Member State with reference to the role of the OECD.

3.9.6 Conclusions on reported national-level priorities for National-level Risk Assessment programmes

As we have seen, there was a great deal of diversity with regard to the suggestions and avenues for improvement, including: a greater understanding of threats and their effects upon society; better management of incidents; greater stakeholder involvement and improved national CIIP frameworks.

Suggestions for the EU level were also proposed, such as the creation of scenario catalogues and provision of guidelines.

4 Conclusions and recommendations

4.1 Conclusions

Concerning national cyber security contexts, we see that there is a great deal of diversity which can make it challenging to provide guidance that would work in all situations. However, this diversity might be seen as a strength, since there might be more adverse consequences for cyber security at the EU level if each country had the same National-level Risk Assessment approach; flaws in the approach would be magnified resulting in extensive policy vulnerability. Understanding national context is likely to have a positive effect upon how the risk analysis is performed (what particular priorities are accorded to different aspects within it) and the best approach to communicate results to senior decision-makers.

Most of the countries that participated in this research used a qualitative or categorical understanding of the severity of risks (low, medium, high) although there were some that had developed quantitative models (e.g. a risk is severe if it affects 1 in 20,000 people). Many countries split the threat actor/agent from the attack means/vector.

We see that there are a diverse variety of types of implementation adopted on a spectrum of centralised to decentralised approaches. This seems to be driven by prevailing contextual factors in a particular country; for instance, the extent to which other stakeholders can be required to follow a particular standard for National-level Risk Assessments or whether this could be successfully accomplished using 'softer' policy mechanisms.

We can see that there are a variety of RA methodologies deployed, including those using qualitative or narrative and quantitative (numerical or mathematical) methods. Some countries have adopted a hybrid approach. Other countries are at an emergent stage with respect to the choice of a particular methodology.

Some key challenges identified include the perception of a lack of a harmonised framework for cyber security (especially with regard to terminology) and the diversity and relative uncertainties of current technical methodologies to perform National-level Risk Assessments. This latter point seems in part to support the evidence generated by this study which aims to provide guidance on the establishment of a National-level Risk Assessment methodology and programme. Other key challenges included those relating to issues of a more systematic nature that affect cyber security, including information sharing.

Many countries are seeking to draw lessons from others regarding establishing or deploying a National-level Risk Assessment programme. The role of international platforms such as ENISA and the OECD would appear to be helpful in this regard. As with many other cyber security issues, establishing good cooperation with the private sector and making sure that responses take account of contexts were also seen as important lessons identified, if not learnt.

Regarding priorities suggested by participants, there was some diversity with regard to the suggestions and avenues for improvement including: a greater understanding of threats and effects upon society; better management of incidents; greater stakeholder involvement and improved national CIIP frameworks. Suggestions for EU-level action were also proposed, such as the creation of scenario catalogues.

4.2 Recommendations

In this section we present our recommendations building upon relevant documents reviewed and the evidence summarised in this report from interviewees and questionnaire.

Recommendation 1: Member States should focus on achieving a better understanding of threats and consequences for society

Member States are recommended to improve their understanding of threats and their impacts upon society by, for example, improving threat analysis mechanisms, creation of appropriate organisational structures to fuse intelligence and disseminating the results of risk analysis to owner-operators of systems with a critical mission.

Recommendation 2: Member States should integrate National-level Risk Assessment into the lifecycle of their NIS cooperation plans and structures

It is recommended that Member States focus upon better integration of national-level risk analysis and management into the cyber incident mitigation priorities, especially in the context of national-level NIS cooperation plans, procedures and structures. The suggestion of further development of horizon scanning could be taken forward at the national level. Specific actions include considering of cross-sector dependencies in National-level Risk Assessment models and frameworks establishing National-level Risk Assessment training and self-assessment measures at sector and national levels.

Recommendation 3: Member States should expand stakeholder involvement and information sharing

The question of how to encourage information exchange between different actors relevant to the execution of National-level Risk Assessments is an important one but there is no easy answer. Member States are recommended to consider the use of different mechanisms (for example, sectoral exercises) to discover fruitful avenues to encourage information exchange. This recommendation could be achieved over the short to medium term.

Recommendation 4: ENISA should develop, test and continuously mature a step-by-step guide for running National-level Risk Assessment Programmes

The evidence gathered in this study, including the outcomes of the panel session during the 2nd International Conference on Cyber Crisis Cooperation and Exercises,[41] indicate there is a clear need for a practical guide to aid Member States with their National-level Risk Assessment programmes. Our recommendation is thus that a step-by-step guide on how to perform a National-level Risk Assessment should be developed by ENISA, tested and maintained. Such a step-by-step guide should be piloted with an EU Member State which is at the start of embarking upon efforts to more formally assess cyber security risks. Such a pilot would set out to trial the use of the guide. Evaluation questions should be specified at the start of the pilot including:

- Who used the guide (in terms of what level of civil servant or administrator)?
- What did users like about it? What did users dislike about it?
- Where was it most effective? And where was it least effective?
- How long did the National-level Risk Assessment programme take to set up when using the guide?
- How many people did it take to run the National-level Risk Assessment programme using the Guide?
- What would you have done differently?
- Are there any issues not covered by the guide which would have been useful to have been included?

[41] https://www.enisa.europa.eu/ccce-conference

Recommendation 5: ENISA should establish a catalogue of scenarios to help Member States with their National-level Risk Assessments

A set of potential cyber threat scenarios could be used by Member States as an off-the-shelf effort to help either kick-start National-level Risk Assessments (for those at the start of the process of setting one up) or for those Member States looking to gather more scenarios or validate existing scenarios. This catalogue could act as a catalyst to help decision-makers get to grips quickly with understanding risks in a controlled 'safe' environment. Work towards this direction that is already being done by ENISA in the areas of the cyber threat landscape,[42] cyber exercises[43] and incident reporting[44] could be used to develop and maintain such a catalogue.

Recommendation 6: A community of practitioners with interest in cyber National-level Risk Assessment should be established by the European Commission

Given the appetite expressed among participants for learning from other countries, another recommendation is to use the momentum gained during the execution of this study to nurture an informal network of National-level Risk Assessment practitioners. This network could share practices and experiences relating to designing, running and operating National-level Risk Assessments in the area of cyber security and CIIP. The establishment of an information-sharing protocol could support this community of interest. The European Commission instruments, such as the NIS Platform[45], would be the most appropriate to implement his recommendation.

Recommendation 7: Exchanging practices in other cross-border risk domains should be reinforced within for example the European Commission's NIS Platform and other activities organised by ENISA

Finally, there are other European institutions that perform similar functions to cyber National-level Risk Assessment in other domains where risks have a cross-border implication. Examples include the European Agency for Operational Cooperation at the External Borders of the EU (Frontex), some of the EU's financially orientated agencies (e.g. the European Central Bank), European Centre for Disease Prevention and Control (ECDC) in the domain of public health and many others. The exchange of perspectives with experts from these other domains and institutions will yield valuable insights into how to support and better facilitate national-level Risk Analysis in a cross-border context across Member States. ENISA's and the European Commission's NIS Platform (see previous recommendation) would be in position to implement this recommendation.

[42] http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment
[43] http://www.enisa.europa.eu/c3e
[44] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/Incidents-reporting
[45] http://ec.europa.eu/digital-agenda/en/news/nis-platform-kick-meeting-working-groups

Bibliography and further reading

ENISA papers

ENISA (2013a). *Report from 2nd ENISA International Conference on Cyber Crisis Cooperation and Exercises, Athens, Greece*. As of 9 September 2013: http://www.enisa.europa.eu/ccce-conference

ENISA (2013b). '*Threat Landscape: responding to the threat environment' Heraklion*. As of February 2013: http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape

ENISA (2013c). *National Cyber Security Strategies in the World*. As of 9 September 2013: *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-in-the-world*

ENISA (2012). *National Cyber Security Strategies Practical Guide on Development and Execution*. As of 9 September 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/cyber-security-strategies-paper

ENISA (2012b). *National Cyber Security Strategies: An Implementation Guide.* As of 9 September 2013: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

ENISA (2011). Inventory of Risk Management/ Risk Assessment Methods. As of 9 September 2013: http://www.enisa.europa.eu/activities/risk-management/current-risk/risk-management-inventory/rm-ra-methods

ENISA (2010). *Cyber Europe 2010 – Evaluation Report.* As of 9 September 2013: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report/at_download/fullReport

EU Legislation and Policy Documents

European Commission (2009). A communication on: A Community approach on the prevention of natural and man-made disasters as of 13 October 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0082:FIN:EN:PDF

European Commission (2010). Staff Working paper on: Risk Assessment and Mapping Guidelines for Disaster Management SEC (2010) 1626 As of 13 October 2013: http://ec.europa.eu/echo/civil_protection/civil/pdfdocs/prevention/COMM_PDF_SEC_2010_1626_F_staff_working_document_en.pdf

European Commission (2013a). Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the union, 2013/0027 (COD). As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2013:0048:FIN:EN:PDF

European Commission (2013b). Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace – JOIN (2013) 1 final – 7/2/2013. As of 9 September 2013: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667

European Commission (2013c). 'Commission Staff Working Document Impact Assessment accompanying the document 'Proposal for a Directive of the European Parliament and of the Council Concerning Measures to ensure a high level of network and Information Security across the Union'

COM (2013) 47 Final; SWD(2013) 31 Final pp. 23–24. As of 9 September 2013: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1669

European Commission (2010). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A Digital Agenda for Europe, COM(2010) 245. As of 9 September 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=com:2010:0245:fin:en:pdf

European Commission (2009). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience, COM(2009) 149 final. As of 9 September 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52009DC0149:EN:NOT

European Parliament & the Council (2013). Regulation (EU) no 526/2013 of the European Parliament and of the Council concerning the European Union Agency for Network and Information Security (ENISA) and repealing Regulation (EC) No 460/2004. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0041:0058:EN:PDF

European Parliament & the Council (2009). Directive 2009/140/EC of the European Parliament and of the Council amending Directives 2002/21/EC on a common regulatory framework for electronic communications networks and services, 2002/19/EC on access to, and interconnection of, electronic communications networks and associated facilities, and 2002/20/EC on the authorisation of electronic communications networks and services. As of 19 July 2013: http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0037:0069:EN:PDF

Other

ANSSI (2010) 'Needs and Identification of Security Objectives'. As of 9 September 2013: http://www.ssi.gouv.fr/en/the-anssi/publications-109/methods-to-achieve-iss/ebios-2010-expression-of-needs-and-identification-of-security-objectives.html

Communications Electronic Security Group (CESG) and Cabinet Office (2009). Technical Risk Assessment HMG IA Standard No. 1. Issue 3.51, October 2009. As of 9 September 2013: http://www.eurim.org.uk/activities/ig/idg/Technical-Risk-Assessment.pdf

Dorfman, Mark S (2007). *Introduction to Risk Management and Insurance* (9th edn). Englewood Cliffs, NJ: Prentice Hall.

Estonian Information System's Authority (2012). 'Three-level IT baseline security system ISKE', 10 May 2012. As of 22 August 2013: https://www.ria.ee/iske-en

Giannopoulos, G, Filippini, R, Schimmer, M (2012). Risk assessment methodologies for Critical Infrastructure Protection. Part 1: A state of the art, *JRC Technical Notes*, EUR 25286 EN-2012 Ispra,

Haimes, YY (2004). *Risk Modelling, Assessment, and Management* (2nd edn). Hoboken, NJ: John Wiley & Sons, Inc.

International Risk Governance Council (2005). White Paper on Risk Governance: Towards an Integrative Approach, IRGC, Geneva 2006. As of 9 September 2013: http://www.irgc.org/IMG/pdf/IRGC_WP_No_1_Risk_Governance__reprinted_version_.pdf

ISO (2012). Standards catalogue. ISO 22301:2012. As of 22 August 2013: <http://www.iso.org/iso/catalogue_detail?csnumber=50038

ISO (2009). Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model. ISO/IEC 15408-1:2009. As of 9 September 2013: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50341

ISO (2008). Information technology – Security techniques – Information security risk management. ISO/IEC 27005:2008. As of 9 September 2013: http://www.iso.org/iso/catalogue_detail?csnumber=42107

Mateski, M et al. (2012). *Cyber Threat Metrics*. Sandia Report 2012–2427, Sandia National Laboratories New Mexico 2012.

Morral, Andrew R, Henry H Willis and Peter Brownell (2011). 'Measuring Illegal Border Crossing Between Ports of Entry: An Assessment of Four Promising Methods.' Santa Monica, CA: RAND Corporation, 2011. As of 9 September 2013: http://www.rand.org/pubs/occasional_papers/OP328

National Academy of Sciences (2010). Review of the Department of Homeland Security's Approach to Risk Analysis. As of 9 September 2013: http://www.nap.edu/catalog.php?record_id=12972

National Institute of Standards and Technology (NIST) (2012). *Guide for conducting risk assessments*. Gaithersburg, MD. As of 9 September 2013: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf

OECD (2012). Joint OECD – Swiss federal Chancellery Workshop on Inter-Agency Crisis Management. As of 9 September 2013: http://www.oecd.org/governance/risk/Speech%20DSG%20Leterme%20-final.pdf

Predd, Joel B, Henry H Willis, Claude Messan Setodji, Chuck Stelzner (2012). 'Using Pattern Analysis and Systematic Randomness to Allocate U.S. Border Security Resources'. Santa Monica, CA: RAND Corporation, 2012. As of 9 September 2013: http://www.rand.org/pubs/technical_reports/TR1211.

Robinson, N, Gribbon, L. et al. (forthcoming, 2013). 'Cyber-Security Threat Modelling Characterisation: a Rapid Comparative Analysis.' PR-171-CATS; RAND, Santa Monica www.randeurope.org/cyber

WEF (2012). *Partnering for Cyber Resilience*, World Economic Forum Report, 2012; Geneva.

Willis, Henry H, Dimitris Potoglou, Wandi Bruine de Bruin, Stijn Hoorens, (2012). 'The validity of the preference profiles used for evaluating impacts in the Dutch National Risk Assessment.' Santa Monica, CA: RAND Corporation, 2012. As of 9 September 2013: http://www.rand.org/pubs/technical_reports/TR1278.

Willis, HH (2007). 'Guiding Resource Allocations Based on Terrorism Risk.' *Risk Analysis*, 27: 597–606.

Willis, HH, ML DeKay, B Fischhoff, PS Fischbeck, HK Florig, MG Morgan (2004). 'Ecological risk ranking: Evaluation of a method for improving the quality of public participation in environmental decision making.' *Risk Analysis*, 24, 363–378.

The White House (2013). *Executive Order on Improving Critical Infrastructure Cybersecurity*. As of 9th September 2013: http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

UK Cabinet Office (2010). *National Risk Register of Civil Emergencies*. As of 9 September 2013: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/211853/nationalriskregister-2010.pdf

List of Acronyms

ANSSI – Agence Nationale de la Sécurité des Systems d'Information (France)

BSI – Bundesamt für Sicherheit in der Informationstechnik (Germany)

CERT – Computer Emergency Response Team

CI – Critical Infrastructure

CII – Critical Information Infrastructure

CIIP – CII Protection

CNPIC – National Centre for Critical Infrastructure Protection (Spain)

DG CNECT –Directorate General Communications; Networks; Content and Technology (EU)

DHS – Department for Homeland Security (US)

ECB – European Central Bank

ENISA – European Agency for Network and Information Security

ETRI – Electronics and Telecommunications Research Institute (Republic of Korea)

GCHQ – Government Communications Headquarters (UK)

HITRAC – Homeland Infrastructure Threat and Risk Analysis Center (US)

KII – Key Informant Interview

IPSC – Institute for the Protection of the Security of the Citizen

IRGC – International Risk Governance Council

ISPC – Information Security Policy Council (Japan)

MSB – Myndigheten för samhällsskydd och beredskap – Civil Contingencies Agency (Sweden)

NAS – National Academies of Science (US)

NCP – National Contingency Plans

NIS – Network and Information Security

National-level Risk Assessment – National-level Risk Assessment (for cyber)

NCSC – National Cyber Security Centre (Netherlands)

NCSS – National Cyber Security Strategy

NISC – National Information Security Center (Japan)

JRC – Joint Research Centre

NIST – National Institute for Standards and Technology (US)

OCSIA – Office of Cyber Security and Information Assurance (UK)

OECD – Organisation for Economic Cooperation and Development

PPP – Public Private Partnership

RA – Risk Assessment

REA – Research Executive Agency (EU)

RIA – Riigi Infosüsteemi Amet (Estonia)

SGDSN – Secrétariate général de la défense et de la sécurité nationale (France)

SME – Small to Medium Enterprise

Annex A: List of organisations involved in the study

Cyprus – Office of the Commissioner of Electronic Communications and Postal Regulation (OCECPR)

Denmark – Govcert.DK

Estonia – Riigi Infosüsteemi Amet (RIA) Information System Authority

European Union – European Council (EU Council)

Finland – Ministry of Transport and Communications

France – Agence Nationale de la Sécurité des Systems d'Information (ANSSI)

Germany – Bundesamt für Sicherheit in der Informationstechnik (BSI)

Greece – National Authority Against Electronic Attacks (NAAEA)

Ireland – Department of Communications

Japan – National Information Security Center (NISC)

Portugal – ANACOM

Republic of Korea – Attached Institute of ETRI

Slovenia – Ministry of Justice and Public Administration

Spain – National Centre for the Protection of Critical Infrastructure (CNPIC)

Sweden – Myndigheten för samhällsskydd och beredskap (MSB) – Civil Contingencies Agency

Sweden – Post and Telecommunications Service (PTS)

Switzerland – Reporting and Analysis Centre for Information Assurance (MELANI)

The Netherlands – National Cyber Security Centre (NCSC)

United Kingdom – Cabinet Office

United Kingdom – Office of Cyber Security and Information Assurance (OCSIA)

United States – Department of Homeland Security (DHS)

Annex B: Key Informant Interview Protocol

Please find below details on ENISA's research project on *National Risk Assessment and Threat Modelling for Critical Information Infrastructures* in which we would like you to participate as an expert interviewee.

Research Outline

At this stage of the project ENISA aims to:

(i) examine empirical evidence on national-level risk assessment and threat modeling for Critical Information Infrastructures (CII) across European Union Member States

(ii) outline risk assessment methodology principles in use by EU Member States that may prove exemplary to others or highlight challenges

Research Deliverable and Approach

The aim of this project is to develop a National Risk Assessment Methodology which could be used by EU Member States. The European Network and Information Security Agency, supported by RAND Europe, is seeking to conduct semi-structured interviews with experts within EU Member States involved in the cyber-security and CII risk assessment fields in order to understand key drivers of these countries' methodologies, policies and approaches that may be valuable to others. This initial phase consists of policymaker interviews supported by documentary analysis. Given your role in the network and information security field in your country and the breadth of your experience, we would be grateful for your input at this initial phase. We propose a short interview with you in person/by telephone addressing the following areas:

- *National co-ordination across cyber-security*
- *Threat modelling characterisation*
- *Approach to risk assessment*
- *Key challenges and next steps*

This annex contains further detail on the broad questions that are relevant to these areas. We are available to organise a meeting in person or by telephone and look forward to hearing from you.

Key topics

National co-ordination across cyber-security

- Which is/are the organisation(s) which has/have the lead in your country in (i) developing the national cyber-security strategy and (ii) outlining cyber-security threats and risks?
- What national-level institutions have responsibility for contributing to threat modelling and risk assessment in CII?
- What are their competences (e.g. inter-agency unit; ministry of Interior; law enforcement; national intelligence agency)?
- How do the lead authority(s) co-ordinate other units with responsibilities in cyber-security domestically? How does the lead authority co-ordinate other units with co-ordinating cyber-security bodies internationally? What learning has been undertaken with regard to risk assessment and threat modelling methodologies?

Threat modelling characterisation

- How are threat actors modelled within current methodologies? What typologies are used? (cf. nation-state; ideological; organised crime)
- What decision processes drive the inclusion of these threat actors? Upon what rationale were they included?
- What process / mechanisms / models are used to characterise threat (expert analysis; computational model; other) and why?
- How is the severity of impact of these threat actors' actions measured? Upon what basis is an understanding and ranking of severity developed?
- What is the influence of other Member State frameworks on characterisation of threat?

Approach to risk assessment

- How are lessons identified and learnt from the conduct of threat assessments across other national-level concerns (cf. crime, terrorism)? What definitions of key terms are used (for example risk) and why were these chosen?
- What approaches to risk are taken (cf. quantitative/qualitative/mixed)
- What tools and methodologies are used to assess risk? What is the rationale for use/rejection of specific tools?
- What is the influence of other states' tools on the risk assessment approach used?
- Is your national methodology public? If so, could you please share it with us?
- Are the results of the assessment made public (partially or in full)?
- If the assessment result is not public, how are the risk owners involved?

Key challenges and next steps

- What are the key challenges faced in threat modelling and risk assessment?
- How do the model and assessment approach used account for and relate to wider National Security priorities?
- What is the frequency, process and depth of review of risk assessment and threat models following implementation?
- How do the risk assessment models affect levels of funding and balance of resource prioritisation?
- What is the maturity of the model used and how do you see it developing? What examples of best practice can you offer to others?
- What would be your recommendations for the EU level in terms of minimum standards in threat modelling and what recommendations for other EUMS?
- What will the model look like in 5 years' time?

Annex C: Questionnaire

Questionnaire: Introduction

National-level risk assessment and threat modelling of (critical) ICT infrastructures and services are essential prerequisite processes in the context of developing and maintaining a national Network and Information Security (NIS) cooperation/contingency plan, which in turn is one of the main pillars of a National Cyber Security Strategy.[46]

As part of the Work Programme 2013, ENISA is undertaking research into national-level risk assessment and threat modelling methodologies used for (critical) ICT infrastructures. The objective in this study is to identify the valuable approaches, practices and challenges that countries have experienced in the methods used for assessing risks of (critical) ICTs infrastructures, the dependencies and challenges. The results of the analysis would help to identify the strengths of the methods used so that all countries in Europe learn from the experiences and practices of others, hoping to close the maturity gap. ENISA is supported to gather evidence for this study by RAND Europe.

Completing this questionnaire

The questions are either yes or no answers or there is space for your comments.

Basic information about you:

Name:	_____
Telephone:	_____
Email address:	_____
Organisation:	_____
Country:	_____
Organisation's role	_____

Cyber Risk Analysis						
PART 1: National Co-ordination						
1.1 Please indicate the extent to which you consider your national-level decision-makers to be familiar with cyber-risk assessment issues (1 = marginal knowledge 5 = very aware)	1 ☐	2 ☐	3 ☐	4 ☐	5 ☐	Comments:
1.2. Existence of national-	Yes	No	Don't know	Comments:		

[46] European Cyber Security Strategy: http://ec.europa.eu/digital-agenda/en/news/eu-cybersecurity-plan-protect-open-internet-and-online-freedom-and-opportunity-cyber-security

level cyber-security strategy	☐	☐	☐	
1.3. Existence of national-level cyber-security risk assessment framework	Yes ☐	No ☐	Don't know ☐	Framework summary:
1.4. Does the cyber security strategy's goals include performing a national risk assessment?	Yes ☐	No ☐	Don't know ☐	Comments:
1.5 Who in your country is(are) the most appropriate entity(ies) to facilitate a national risk assessment?	_____			
1.6 Please describe the challenges you encountered and how you overcame them?	Defining terminology ☐			
	Moving from a reactive to a pro-active approach ☐			
	Understanding the domain ☐			
	Competencies for RA ☐			
	Identifying sources of information ☐			
	Quality of information ☐			
	Limited public-private information exchange ☐			

PART 2: Cyber-Related Threat Modelling and Risk Assessment

2.1. Does the country recognise and share standardised definitions regarding cyber threats and risks?	Yes – national ☐	Yes – international ☐	No ☐	Don't know ☐	Comments:
2.2. Has the country undergone a process to define and share understanding of key terms such as risk, threat and vulnerability in a cyber-context?	Yes ☐		No ☐	Don't know ☐	Describe/Comments:

2.3 Are Critical Information Infrastructure assets identified?	Yes ☐	No ☐	Don't know ☐	Briefly summarise:
2.4. Is there a national Critical Information' Infrastructure Protection (CIIP) strategy?	Yes ☐	No ☐	Don't know ☐	Comments:
2.5 Please indicate whether your country adopts a centralised or decentralised approach to risk assessment?	Yes ☐	No ☐	Don't know ☐	Comments:
2.6 Are dependencies between cyber; physical and personnel risks acknowledged?	Yes ☐	No ☐	Don't know ☐	Comments:
2.7 How are they addressed?				
2.8 Have you or do you plan to identify and engage stakeholders on cyber risk assessment?	Yes ☐	No ☐	Don't know ☐	Comments
2.9 If so, which ones:	National telecommunications regulatory authorities	☐		
	National/governmental Computer Emergency Response Teams (CERTs)	☐		
	National law enforcement agencies	☐		
	Other	☐		
2.10 Please briefly summarise this process (who, how, duration)?				
2.11 Please indicate which challenges you have encountered in relation to cyber risk analysis				
Generic Risk Assessment				

PART 3: Generic Threat Modelling and Risk Assessment				
3.1. Do you have an estimate on the costs of the national Risk Assessment process?	Yes ☐	No ☐	Don't know ☐	Comments on estimated costs:
3.2. Do the results of the risk assessment affect resourcing / funding?	Yes ☐	No ☐	Don't know ☐	Comments:
3.3 Do risk assessments broadly account for threat, vulnerability and consequence?	Yes ☐	No ☐	Don't know ☐	Comments:
3.4 Please describe the risk assessment methodologies/models that you use or are considering to use:				
3.5 Is observed data at national level on the prevalence of threats and vulnerabilities tracked?	Yes ☐	No ☐	Don't know ☐	Comments:
3.6 Are you planning to test and/or validate the risk assessment methodologies considered?	Yes ☐	No ☐	Don't know ☐	Briefly describe the process:
3.7 Is the risk assessment benchmarked against approaches used by others?	Yes ☐	No ☐	Don't know ☐	Comments:
3.8 Do you consider the risk assessment methodology drawing from other countries?	Yes ☐	No ☐	Don't know ☐	Comments:
3.9 Is expert judgment used to assess risks?	Yes ☐	No ☐	Don't know ☐	If yes how?
3.10 Is uncertainty about threats integrated into the analysis?	Yes ☐	No ☐	Don't know ☐	If yes how?
3.11 Are threat scenarios considered?	Yes ☐	No ☐	Don't know ☐	

3.12 Please indicate all that apply	Force Majeure (seismic; wind; heat etc) ☐					
	Technical (e.g. random failure of hardware or software) ☐					
	Deliberate / adversary based (organised crime; nation-state; lone individual) ☐					
	Human error (mistakes or misconfiguration) ☐					
	Secondary (e.g. maintenance; organisational policy;) ☐					
	Other ☐					
	Please describe _____					
3.13 Which organisation are risk assessment results/outcomes communicated to?	Government elected officials ☐					
	National Intelligence Machinery ☐					
	Foreign Affairs ☐					
	National-level law enforcement (e.g. Cybercrime Units) ☐					
	Private sector Critical National Infrastructure owners ☐					
	Academia ☐					
	Other ☐					Comments
3.14 Please indicate which mechanisms you employ or are considering to extract lessons learned	After Action Reviews ☐	Day after exercises ☐	Seminars ☐	Knowledge exchange programs ☐	Other ☐	None ☐
3.15 Please indicate the participants in such mechanisms	Govt Partners ☐	European ☐	Non-European ☐	Other (please describe) ☐	_____	
3.16 Please briefly describe the nature and frequency of such mechanisms	_____					
PART 4: Challenges and Next Steps						
4.1. Is there monitoring of international developments in risk analysis?	Yes ☐	No ☐	Don't know ☐	Examples/Comments:		

4.2 Do you engage with international developments in risk analysis?	Yes ☐	No ☐	Don't know ☐	Examples/Comments:
4.2. Have minimum standards been set for desirable levels of security?	Yes ☐	No ☐	Don't know ☐	Examples/Comments:
4.3 Are you open to explore new approaches to measuring threat and capturing impact being considered?	Yes ☐	No ☐	Don't know ☐	Examples/Comments
4.4 What are the key challenges faced in threat modelling and risk assessment?	_____			
4.5 Please describe the process used or considered for validating your risk analysis approaches	_____			
4.6 Priorities for EU: Please indicate your top five priorities for EU level action in the area of cyber risk assessment and whom you think should take these forward:	Threat catalogues	☐		
	Policy guidance	☐		
	Scenarios	☐		
	Methodologies	☐		
	Experts to help validate work	☐		
	Other	☐ Comments:		
4.7 What do you consider your model of risk assessment looking like in 5 years time?	_____			
4.8 Further remarks	_____			

ENISA
European Union Agency for Network and Information Security
Science and Technology Park of Crete (ITE)
Vassilika Vouton, 700 13, Heraklion, Greece

Athens Office
1 Vasilissis Sofias
Marousi, 151 24, Athens, Greece

PO Box 1309, 710 01 Heraklion, Greece
Tel: +30 28 14 40 9710
info@enisa.europa.eu
www.enisa.europa.eu