Evaluating a national cyber security strategy

1 Introduction

The February 2013 the European Commission's Cybersecurity Strategy[1] set out ambitious objectives. One of those objectives is to ensure that each Member State will possess a National Cyber Security Strategy to address cyber security risks and challanges. However, in the current times of economic austerity, it is ever more important that such strategies be evaluated to determine whether impact is achieved.

In continuance to ENISA's work on National Cyber Security Strategies (NCSS) and following the publication of a best practice guide in 2012[2], this short paper presents an early scoping of evaluation in the context of NCSS. The goal is to provide a preliminary overview of evalution in NCSS to inform further discussion and debate about the preparation of a possible, more formal framework for measuring key performance of NCSS.

This report will be of interest to: those in the ENISA evaluation of NCSS Expert Group, policymakers at the national and European level (especially those involved in drafting, preparing or implementing NCSS) and other interested experts as well as researchers.

[1] http://eeas.europa.eu/top_stories/2013/070213_cybersecurity_en.htm
[2] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/national-cyber-security-strategies-an-implementation-guide

2 Towards a national evaluative logic model

2.1 Evaluation in the ENISA NCSS lifecycle

The strategy lifecycle model is illustrated in Figure 1. As the figure indicates, the evaluation activities refer to both one-off evaluations and on-going/periodical evaluation and monitoring activities. Within this framework, strategies are supposed to be evaluated both at the programme level and from the point of view of the ultimate outcome, using a range of methodologies including cost-benefit analysis, benchmarking, descriptive statistics, stakeholder consultation and others. However, as all these methodologies address particular aspects of the strategy, a clearly outlined needs to accompany the strategy.

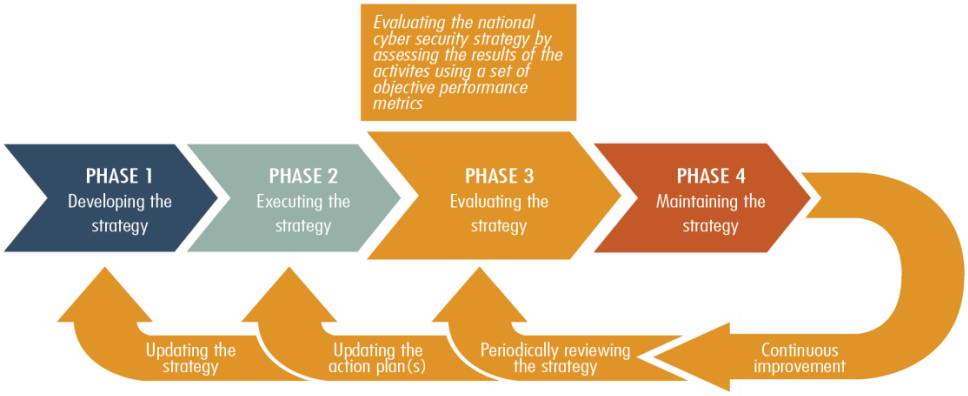

Figure 1 Lifecycle of a national cybersecurity strategy (ENISA 2012)

The 2012 ENISA Best Practice guide on cybersecurity lists the following principles to be taken into account when designing an evaluation framework:

- *Define the scope of the evaluation, the key objectives, the expected outcomes and the periodicity of it.*
- *Implement the 'Segregation of duties' principle: assign to an independent entity, a supervisor or a trusted third party (other than the national cyber council) the task of evaluating the effectiveness of a national cyber-security strategy and its activities (e.g. a national cyber security council).*
- *Empower the independent entity with the appropriate mandate, role and responsibilities to succeed in this operation.*
- *Encourage and offer incentives to stakeholders to be involved in the evaluation process.*
- *Evaluate not only the strategy but also the individual tasks of it.*
- *Follow both a quantitative and qualitative approach giving emphasis on both impact and results.*
- *Perform an internal/self-impact assessment for each activity of the strategy taking into consideration the opinion of the stakeholders.*
- *Perform an external impact assessment for each activity of the strategy taking into consideration the opinion of external and/or affected users/communities.*
- *Evaluate each activity against the action plan and key performance indicators (KPIs) agreed when the activity kicked off; evaluate KPIs through questionnaires (online) and polls within the stakeholder community.*
- *Create a data collection scheme for obtaining relevant data for the evaluation of the strategy and the action plan. Effectiveness of the strategy should be measured at all levels. The data collection process should become comprehensive.*

- *Identify lessons, good practices and bad practices from the internal and external impact assessment as well as the evaluation of each activity.*
- *Prepare an analytical evaluation report describing the achieved results and the expectations for the next evaluation.*
- *Carry out benchmarking studies in order to compare strategies between different Member States. The outcomes of a benchmarking study can be used to identify areas of improvement.*

2.2 Outline of an evaluation model

The key components of an evaluation model, based on our research are presented in this section:

- 'Resources' or 'Inputs' into the programme that is being implemented (e.g. financial, staff, physical, relational resources needed to pursue the NCSS' objectives);
- 'Activities' or 'processes' through which the programme aims' and objectives' are being pursued (e.g. activities related to increasing awareness etc) ;
- 'Expected outputs' – i.e. direct shorter term achievements (e.g. influences on policy audiences, publications, etc.); and
- 'Expected outcomes and impacts' – i.e. longer-term expected consequences (e.g. improved cybersecurity/ resilience in the country and in Europe).

In order to synthesise the links between these elements and how they contribute to the ultimate outcome of an NCSS and cyber policy, we have developed a logic model that summarises the relationships between inputs/resources, processes, outputs and outcomes. After the implementation of this model, the key performance indicators (KPIs) emerge.

While none of the strategies examined for this study presents an integral view of all the elements included in the draft logic model, we illustrate each step with examples that are separately available in different documents. Figure 2 summarises the elements of the logic model for NCSSs.

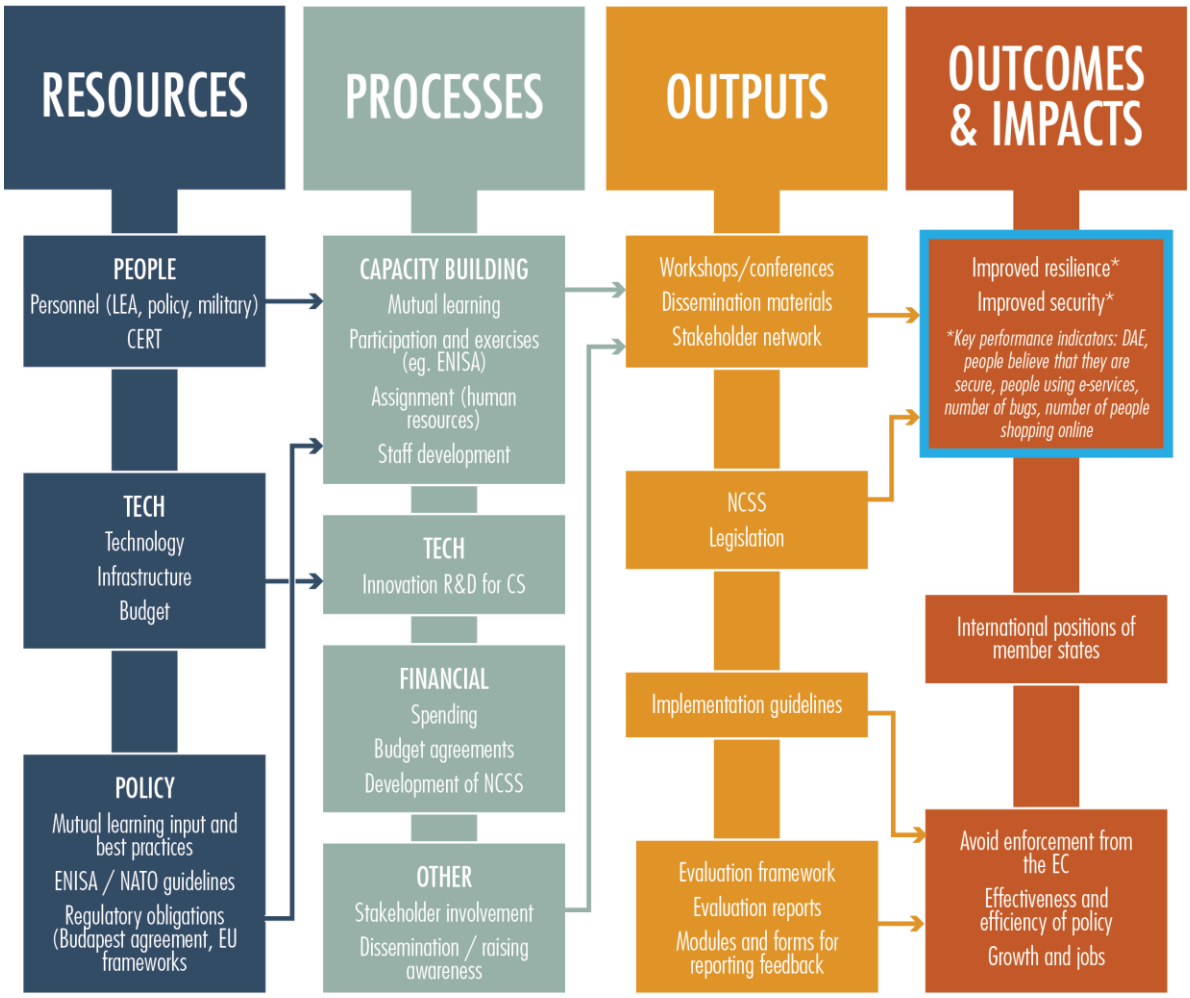

Figure 2 Logic model for NCSS

2.2.1 Inputs

Inputs indicate the resources that are made available for the implementation of the NCSS at both strategy and programme level, which can be leveraged to pursue the objectives of the NCSS. These include financial, human and relational resources, among others.

Example of Input

The **UK** cybersecurity framework[3] is a good example of resources explicitly dedicated to cybersecurity. With the publication of the second cybersecurity strategy, a total of £ 650 million have been earmarked to support the actions envisaged in the strategy and the implementation plan, with £383 million being allocated to intelligence tasks. The Home Office was allocated 10 per cent of this budget (or £65m); while the Ministry of Defence got 14 per cent (£91m) and the government kept 10 per cent to build secure online services. However, the Department of Business was allocated just 2 per cent (£13m), earmarked on working with the private sector to improve resilience, inferior to the five per cent (£32.5m) allocated to the Cabinet Office to co-ordinate internet security

[3] Reference

initiatives.[4] Such expenditure, however, is not always separately identified in departmental budgets and is not therefore readily quantified. [5]

2.2.2 Processes

Processes are the core interventions though which the outputs of the project are achieved. It is fundamental that they are defined in a way that encompasses all inputs and the projected outcomes. In most cases, the processes are described and periodically updated through the implementation plans of the national strategies.

In some cases where centralised funding is available, central government bodies are more heavily involved in defining the processes, while in countries with more decentralised systems and where cybersecurity activities are financed out of the standing budget lines of the entities involved, processes are designed by the departments themselves.

Example of Processes

The recently adopted, second **Dutch** cybersecurity strategy[6] articulates its vision around processes and outcomes of the actions linked to its strategic goals.

For instance, it establishes that *"Within the framework of the protection of critical infrastructure, the government, working with vital parties, will identify critical ICT-dependent systems, services and processes. These efforts are linked to a programme that will establish basic security requirements on the basis of risk analyses."*

Another example is the process of setting up new entities within the policy environment, for instance similar to the **Austrian** Operational Coordination Structure proposed in the national cyber strategy.

"Building on and taking advantage of existing operational structures, a structure for coordination at the operational level will be created. It will serve as a platform for preparing a periodic and incident-related Cyber Security Picture and for deliberations on measures to be taken at the operational level. Furthermore it will provide an overview of the status quo in cyberspace by collecting, compiling, evaluating and passing on relevant information. The economic sector should also be involved appropriately and on an equal footing.[7]"

2.2.3 Outputs

Outputs are the direct results of programme activities. These are usually linked to key performance indicators as they are relatively easy to measure quantitatively and qualitatively, and can be audited to ensure sound implementation. While the general objectives of cyber strategies are important to keep present when evaluating the strategy, they are usually defined in vague terms. Therefore there is often a lack of a clear understanding of how these objectives are measured or through which specific processes the strategy conducts in the realisation of the objectives. As implementation plans and reports are usually separate documents from the strategy, and are usually classified, a complete in-depth evaluation of a strategy needs to have access to all these documents.

Example of Output

[4] John Leyden, "Spooks take the wheel in UK's £650m cyber-war operations", *The Register*, , 28th November 2011 , http://www.theregister.co.uk/2011/11/28/cyber_security_strategy_analysis/ , accessed 22 November 2013

[5] NAO, *UK Cyber review*, 2013, http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

[6] Government of the Netherlands, the Ministry of Security and Justice, Netherlands National Cyber Security Strategy, *From Awareness to Capability*, 2013

[7] Republik Österreich, *Austrian Cyber Security Strategy*, 2013, p.10, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

Implementation reports usually measure outcomes, for instance by listing the number of individuals that have taken part in a course; whether a certain strategic document has been adopted; or whether a new entity has been set up.

An example of output is the establishment of a national CERT in line with European guidelines, which is often enshrined in the national strategies. For instance, the **Czech** strategy states:

"Because of threats faced by ICTs, security and reliability of information and communication systems of the critical national infrastructure ranks among top priorities of the Czech government. To this end, the government intends to establish a government coordination agency that could immediately respond to computer incidents, namely a Computer Emergency Response Team (hereinafter "CERT"). The agency will be a part of both the national and international cyber threat early warning systems.[8]

2.2.4 Outcomes

Outcomes are the longer-term expected results of the strategy, exerted over several years. In contrast to outputs, which are often tangible and easily quantifiable, outcomes are expressed in more complex socioeconomic terms and cannot easily be measured. Furthermore, the difficulty of clearly identifying the links between the preceding elements of any implementation plan (i.e. inputs, processes and outputs) to the longer-term outcomes has been identified, as the realisation of these hinges on multiple external factors.

Example of Outcome

An example of outcome often found in national strategies relates to the positioning of a given country in terms of competitiveness of its cybersecurity infrastructure. While in some cases an increased level of security is framed as a means to ensure international leadership of the country in the area (Finland, Estonia), some other countries (e.g the UK)use this to be constituted one of the least vulnerable targets to criminal attacks (UK cyber strategy 2012).

The introduction of the Finnish strategy summarizes its vision in terms of strategic outcomes:

- *"Finland can secure its vital functions against cyber threats in all situations.*
- *Citizens, the authorities and businesses can effectively utilise a safe cyber domain and the competence arising from cyber security measures, both nationally and internationally*

By 2016, Finland will be a global forerunner in cyber security preparedness and in managing the disturbances created by these threats"[9]

2.3 Key Performance Indicators

Incorporating KPIs in the strategy is the evaluation steps need to be taken when assessing the progress towards the already set aims and to learn from the experience.

In order to gain a coherent grasp on the efficacy and efficiency of the strategy and the implementing actions policy makers need to find a way to frame each of the elements in a 'measurable' way. This can happen either by defining what outcomes an observer would expect to see at a certain stage of implementation or by including specific output indicators of the extent to which certain activities

[8] Government of the Czech Republic, *Cyber Security Strategy of the Czech Republic for the 2011 – 2015 Period*, Paragraph 18, p. 8, http://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss/CzechRepublic_Cyber_Security_Strategy.pdf

[9] Secretariat of the Security Committee, *Finland's Cyber Security Strategy*, Government (Resolution 24.1.2013), 2013, pp. 3, http://www.defmin.fi/files/2378/Finland_s_Cyber_Security_Strategy.pdf

have been delivered (e.g the number of workshops held). Some initial examples of KPIs and data sources can be found in Table 3 below:

Table 3 Key performance indicators and how to measure them

	Example of KPIs	Example of units of measurement
Inputs / resources	• Human resources; • Financial resources allocated at government and department budget level; • International alliances.	• Man- hours allocated to task; • Budgets; • Number of international organisations involved; • Number of MoUs with other governments.
Processes	• degree of involvement of different stakeholders • pre-defined milestones in the process have been reached.	• Number of stakeholders involved in public consultations; • Annual activity reports;
Outputs	• number of people trained; • setup of cyber security governmental bodies; • scale of investment in R&D; • adoption of legislation; • Awareness raing campains and NIS in education; • percentage of businesses having implemented a cybersecurity strategy.	• Reports from training programs; • Activity reports from new bodies; • Numbers of campains, impact spread; • Legal acts; • National and industry statistics.
Outcomes	• Level of public trust in cyberspace; • Internationalisation of digital economy.	National, international and industry statistics.

KPIs work best when tailored to the context of the individual policy or strategy in order to provide relevant information to policymakers. To this end, they are often defined through a dialogue within the organisation, through asking questions regarding the ultimate purpose of elements of the strategy and how best these can be captured. Furthermore, from a governance perspective it can be useful for the strategy if KPIs are defined so that they:

• are controllable by the owner;

• make a significant impact on current or future performance;

• are aligned to the strategy; and

•can have a pre-defined "level of success" where the desired outcome is reached. [10]

However, using KPIs also presents challenges at each stage of the logic model. In particular in a field with the characteristics of cybersecurity, establishing quantitative success indicators can be an arduous task that goes beyond the goals of the policy itself. Furthermore, KPIs can risk steering the process towards an outcome-based approach and distort the attention from the overall context in which the policy operates. Communicating and coordinating evaluation and monitoring across organisations can challenge the implementation of comprehensive plans which build on KPIs.

3 Fitting evaluation process into the Cyber Security Strategy lifecycle

In this chapter we elaborate how evalution fits into the broader framework of the cycle of a National Cyber Security Strategy, based on the key informant interviews conducted for our study. In the interviews conducted for the present study we gained in-depth information about the role that evaluation and monitoring plays in national cybersecurity landscapes. Some of the insights are summarized below.

- **Political priorities and recent events drive the formulation of strategies**
  The role of evaluation and the priorities against which the implementation of national strategies is evaluated is not always closely linked to the original motivations that have informed the formulation of the strategy itself. As it emerged, setting up a strategy is often driven by a need to adapt the cyber strategy to updates the national risk management framework i.e. in the UK the update of the strategy was driven by the characterisation of cybersecurity as a Tier 1 threat in the revised national risk assessment (UK); a sense of inadequacy of the national defence strategy in the face of emerging technological threats (FR); particular large-scale events that impacted on political priorities (EE); or by the desire to strengthen the international standing of the country in cybersecurity (SK). Hence the implicit interpretation of "resilience and security" may vary between the countries, as do the implicit assumptions about the goals, enablers and challenges of the frameworks.
- **The main contribution of the strategies to resilience is often perceived in creating a framework that brings together stakeholders**
  One of the added values of the development of a national strategy is the potential of the framework created to encourage dialogue between levels of and different stakeholders. For instance, the cooperation between levels of government can take the form of periodical reports to Parliament by the organisation responsible for overseeing the implementation of the strategy, on a yearly or biannual basis (UK, AT). Such network-building processes are further reinforced by the multidisciplinary nature of cybersecurity, central funding where applicable and the consequent need for government departments and stakeholder organisations to act in a coordinated manner. However this aspect is often not captured in the evaluation of the strategy.
- **Evaluation practices and key performance indicators are most often linked to inputs and outputs and rarely to long-term outcomes of the process**.
  Independently of the type of funding of cybersecurity programmes (centralised or decentralised), the programmes are subject to the spending review processes of the individual Member States and to those established at the European level. Therefore, a number of KPIs found in the evaluation and review processes of most strategies are related to the efficiency of these programmes from a financial audit viewpoint. Other KPIs are associated with the individual actions implemented under the programme, and serve for

[10] SAS, *Designing KPIs For Improved Public Sector Performance*, SAS white Paper, 2013

internal and programme-level audits. These KPIs most often focus on outputs, such as the number of training courses or curriculum changes in public education; outreach initiatives or legislative processes or indicators related to dissemination such as the number of businesses downloading cybersecurity guidelines (UK).

Even where outcomes are included in the strategy and formulated in terms that would enable a quantitative measurement, the difficulties in establishing a clear causal link between the strategy and the societal/economy level developments limit the credibility of these aspects in the evaluation framework (FR). That said, some strategies concentrate on measurable aspects of these outcomes- for instance on success in combating incidents rather than quantifying harms and costs (UK).

The fact that most outcomes are expected to realise their full impact on the medium to long term, rather than the short-to-medium term (which is often the horizon of evaluations) raises further challenges to including these in reviews (UK). In fact, in some strategies the KPIs regarding society-level benefits (e.g. indicators of systemic trust such as the number of people shopping online) have not been included in the first period of implementation and are scheduled to be developed for the second cycle of the NCSS (AT). Furthermore, our interviews indicated that quality-related indicators are also often absent from evaluation frameworks, and that this lack of attention to the quality of the activities is often seen to risk jeopardising the outcomes (SK, EE).

Most countries have some kind of review and evaluation process in place. However, these are often not easily identifiable as they are often not explicitly linked to the strategy, and rather form part of a wider, government-level approach to programme and policy evaluation and spending reviews. For instance the UK National Audit Office has recently published a detailed evaluation on the financial efficiency of the actions taken thus far under the Government Cybersecurity Strategy[11].

- **Key challenges in the implementation and evaluation of NCSSs are technology, internal political landscape and financial resources**

  The political context in which the strategy is implemented and updated is important; this context may determine the level of priority that the strategy assumes and subsequently the amount of attention and resources dedicated to it. In the same context, the financial and human resources available for evaluation and monitoring also appear to diverge between Member States.

- **The EU framework, EU funding as well as the internal political constellation and investment in human resources are among the key enablers**

  In particular, the international context and EU policy drive, together with the national political drive towards a prioritisation of cybersecurity that has been acknowledged by several interviewees to be an important element in domestic agenda-setting (UK, SK, EE). Furthermore, EU funding and the corresponding evaluation obligations in the countries receiving funds earmarked for critical information infrastructure (CII) development (SK) appear to be an important factor in establishing the demand for follow-up in the programmes. Finally, the availability of human resources is also a significant enabler in putting in place an evaluation framework.

[11] NAO UK Cyber review, 2013, http://www.nao.org.uk/wp-content/uploads/2013/03/Cyber-security-Full-report.pdf

4 Conclusion

As discussed above, defining and framing outcomes (or benefits that can be observed upon implementation of an NCSS) is one of the most challenging aspects of the setting up the logic process of a cybersecurity strategy. One of the most relevant ultimate outcomes of a strategy or a national cybersecurity policy is to increase resilience and security of cyberspace (at the national and supranational levels). However, the meaning of "security and resilience" is open for further interpretation, and the interpretation chosen influences the key performance indicators, as well as the processes, inputs and outputs that can be assigned to these goals. Some aspects to define outcomes of a strategy in the national cybersecurity landscape are:

- Human security [12]. The EU Cyber security strategy reflects the attention to principles of the human security doctrine that characterises "hard" security policy. It expressly notes that cyber security is in the service of ensuring access for all; the protection of human rights; democratic governance; and shared responsibility.
- Confidence in digital transactions. Here we concentrate on the willingness of businesses to be active in the digital market space. In Europe, despite a persistent regional divide, businesses already appear as having more confidence to transact with each other than individual customers. Some indicators that can be used as proxies in evaluation processes could be, for instance, linked to measurements of growth in B2B exchanges.
- Citizen/ consumer trust. In this context we refer to systemic trust as an expression of the trust of citizens in societal institutions, which include not only trust in their governments but also trust in the broader frameworks governing our lives, such as the market economy (which includes digital markets), [13]In the digital environment this concept is fundamental, in particular as a high level systemic trust can facilitate engaging with cyberspace in novel ways for users, where they cannot rely on experience-based trust.
- Critical information infrastructures protection: Critical infrastructure providers are important intermediaries in the operationalisation of national cybersecurity strategies. While some data on updates can be obtained from companies manufacturing the software, it can be difficult to distinguish between purchases / downloads made by CIIPs and other companies. Instead, due to the existence of mandatory reporting obligations, existing secondary indicators can be used as proxies for the level of security and resilience of the CI.
    - One such source of information – bearing in mind the limitations implicit in the setup of reporting structures defined with legislation[14] - can be trends deduced from the reports filed under **mandatory reporting regimes** (established in Article 13a of the 2009 Telecommunications package or the proposal for a Network and Information Security (NIS) Directive.
    - Another potential proxy for illustrating improvements in the levels of security can be gauged through monitoring trends in the number and characteristics of incidents reported to governmental or national CERTs.

[12] Council of the European Union, *A Human Security Doctrine for Europe: The Barcelona Report of the Study Group on Europe's Security Capabilities*, http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/solana/040915CapBar.pdf

[13] Schweer, M., & Siebertz-Reckzeh, K., Personal, "Systemic and Transsystemic Trust: Individual and Collective Resources for Coping with Societal Challenges", In *Mindful Change in Times of Permanent Reorganization*, 2014, (pp. 225-243), Springer Berlin Heidelberg.

[14] European Parliament, *Data and Security Breaches and Cyber-Security Strategies in the EU and its International Counterparts*, 2013, http://www.europarl.europa.eu/RegData/etudes/note/join/2013/507476/IPOL-ITRE_NT(2013)507476_EN.pdf

At the same time, all the listed data sources have specific limitations and can be used in evaluation only if the caveats resulting from the areas covered by the indicators, their method of sampling and data collection and the potential conflicts of interest that can pertain to data collected and distributed by commercial actors, such as companies producing cybersecurity software, are taken into account. Ideally, evaluation activities would take into account these aspects when defining the set of KPIs used to assess the three aspects of resilience and security outlined above.