The 2015 Report on National and International Cyber Security Exercises

Survey, Analysis and Recommendations

FINAL

1.0

DECEMBER 2015

www.enisa.europa.eu European Union Agency For Network And Information Security

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.

ENISA project team

Adrien OGEE (Contributor)
Razvan GAVRILA (Project manager and main editor of this study)
Panagiotis TRIMINTZIOS (C3 program manager - contributor)
Vangelis STAVROPOULOS (Reviewer)
Alexandros ZACHARIS (Reviewer)

Contact

For contacting the authors please use c3@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

Acknowledgements

ENISA would like to acknowledge the valuable involvement of SECANA AB to this study, in particular the contributions of Baris Uckan Färnman, Mats Koraeus and Sarah Backman. ENISA would also like to express its gratitude to the wider cyber exercise community that validated some of the early hypotheses that lead to this study.

ISBN: 978-92-9204-158-8, **DOI:** 10.2824/627469

Table of Contents

Executive Summary

The purpose of this study is to gather and analyse a primary dataset as the first step towards an EU-wide dataset on cybersecurity exercises, and to create a model for continued reporting on such exercises. The study is the first step towards the larger goal of using the dataset as a resource for planning and collaboration between nations and agencies interested in cybersecurity exercises.

A dataset consisting of over 200 cybersecurity exercises and specialised literature such as after-action reports and previous studies have contributed to the analysis.

The findings show a continuous and accelerated increase in the total amount of exercises held after 2012, as well as an increase in the number of cooperative exercises involving private and public actors. This indicates that it is not just a matter of public agencies running more exercises, but also of more actors benefitting from these exercises.

The study also reveals that many cybersecurity exercises focus on exploring new structures and collaborations, rather than consolidating or building on established ones. Even though this exploration is an important step towards reaching consolidation, it might be in the best interest of the participants to take the next step of establishing procedures.

Finally, the public-affairs aspect, and in particular the explicit goal of educating both the public and decision-makers, is left relatively unexplored in much of the exercise design and planning. While there are undoubtedly links between an increased awareness of cybersecurity issues and an increased number of exercises, this exact nature of this link requires closer inquiry and requires a rather different analytical lens. Nevertheless, as an understanding of cybersecurity issues becomes more and more relevant for an increasingly larger audience, the opportunity to reach such an audience is often missed.

Based on our analysis, this report provides four main recommendations that would help to increase the quality of future cybersecurity exercises.

1. **ENISA should establish a common ground for the exchange of best-practices regarding cybersecurity exercise development**

The dataset developed in parallel to this analysis report has the potential to become a common ground for information and knowledge sharing regarding cyber exercises. ENISA should further develop this dataset by setting a clear focus on experience sharing, knowledge and lessons learned from exercise activities.

2. **Member States should contribute to the cybersecurity exercises community**

In order for the ENISA Cyber Security Exercises Dataset to be a source of valuable information regarding exercises, best practices and methodology, it requires input from the community. We urge all actors involved in exercise activity to contribute to the ENISA Cyber Security Exercise Dataset by providing input during the planning and the evaluation phase of future exercises.

3. **ENISA should produce an Analysis report bi-annually**

The 2012 and the 2015 Analysis report teaches us a lot about the developments within the field of cybersecurity exercises and what the trends have been and where trends are heading. By making this Analysis report a bi-annual publication, it allows for further knowledge spreading, but also, better follow-up

on what the impacts are from the developments within the field. We recommend that the Analysis report becomes a bi-annual publication and that the dataset is updated in accordance with the Analysis report drafting including input from experts in the community.

4. The MS and ENISA should co-develop a European exercise calendar

There is an increased number of cybersecurity exercises, an exercise calendar would help in visualising the exercises being held and would increase awareness amongst stakeholders in Europe and beyond. ENISA should develop the exercise calendar and attach it to the exercise dataset.

List of figures

1. Introduction

Since 2009, after identifying and stating the growing importance of cyber exercises, ENISA has worked continuously to support the development of cybersecurity exercises in Europe and support stakeholders involved in cyber exercises in Europe. This report extends the results of an initial stocktaking of national and international cyber exercises conducted in 2012. [1] It provides an updated picture on the development of cybersecurity exercises worldwide since 2012.

The purpose of the ENISA 2012 report on cybersecurity exercises was to provide a snapshot in time of the state of affairs within the cybersecurity exercises sphere, as well as to provide a general historical overview of the preceding decade. The report aimed to support European and international bodies involved in cyber exercises by providing lessons learned as well as recommendations as well as to increase the quality and number of cyber exercises.

The 2012 report identified a number of trends in cyber exercises, suggested the organisation of more exercises, more cross-border collaboration, and a more inclusive participation. At the same time, the report illustrated the overall pattern of deficiencies in exercise management tools, the correlation between methodological planning, monitoring and evaluation of an exercise. ENISA recommended in the report to increase the focus on developing tools and methodologies for both informed planning and improved learning from future exercises.

The 2015 report on this topic tries to extend the findings of the 2012 study by a) bringing the collected exercise data up-to-date, i.e. covering the period 2012-2015, and b) validating the lessons learned and the proposed actions.

1.1 Aim and Purpose

The primary purpose of this study is to gather and analyse a dataset of cybersecurity exercises, drawing conclusions on the evolution of cyber exercises in Europe and beyond. In addition, through this study ENISA would like to establish a model for regular analysis of such exercises in the future. The study itself is only the first of four conceptual phases towards the larger goal of using the exercise dataset as a resource for exercise planning, collaboration between nations and agencies, more efficient and effective training of cybersecurity professionals and decision-makers. While the second, third, and fourth phases are beyond the scope of this report, the end goal of increasing cooperation and knowledge sharing in the field of cybersecurity exercises still very much influences the aim and purpose of the report.

Overall, this first phase is characterised by an exploration of what data is relevant for further study and of what data currently exists on cybersecurity exercises. The intent is to identify the methodological pitfalls that might taint or skew both the data gathering itself and the analysis of the data, as well as to seed the dataset with recent information from stakeholders in the cybersecurity field, so as to act as a foundation for a longer-term analysis over time.

[1] ENISA Report on National and International Cyber Security Exercises, survey, analysis and recommendations. 2012. Available at: https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012

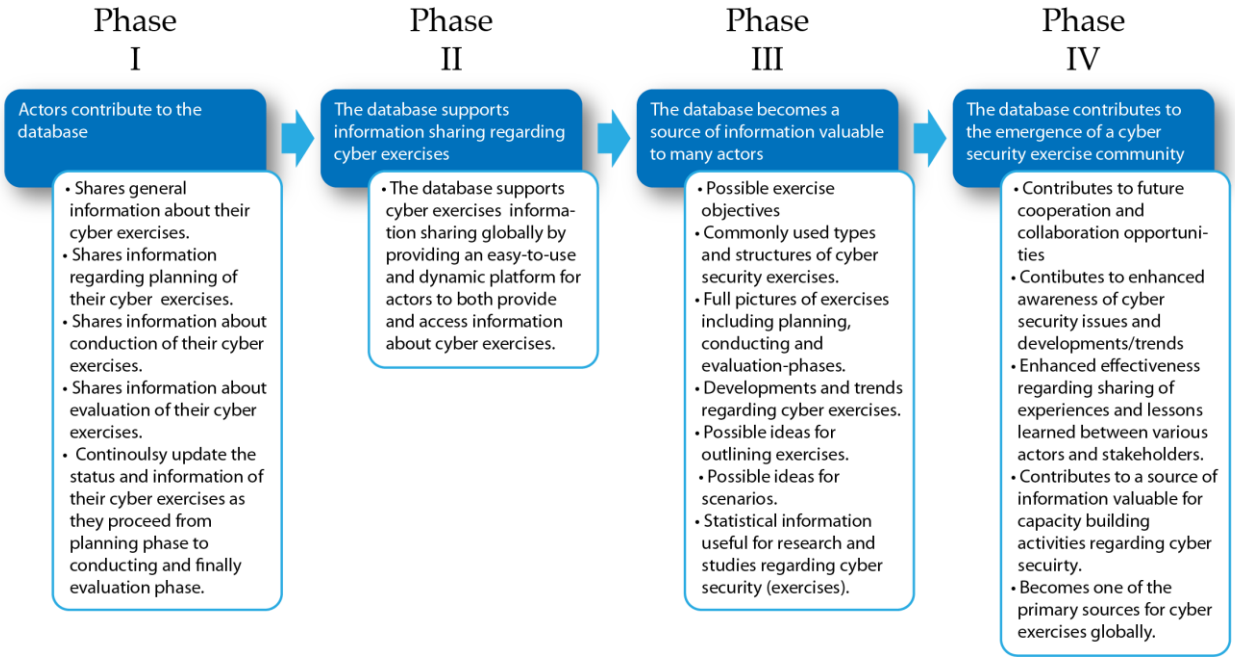

Figure 1: Phases of establishing a shared exercise knowledge platform

The dataset and the methodology created in **Phase I** will then act as a foundation for future EU-wide efforts to create a central repository of exercise information that can be shared among relevant stakeholders in Member States. **Phase II** will validate and harden the dataset, as well as to develop user-oriented interfaces to allow the stakeholders to contribute to benefit from the information in it. **Phase III**, purpose of information sharing, allows interested parties to identify trends in the field and to exchange best practices in exercise planning and methodologies. Finally **Phase IV** will help with widespread, full-fledged cooperation in exercises, leading to more opportunities for combined exercises within the community.

1.2 Structure of the report

This report begins by presenting a short history of cyber exercises and of cyber exercise studies. The key input to this being the 2012 ENISA report on cyber exercises[2] which acts as a driver for this extended study, which makes up the second and third section of this analysis.

The next chapter presents the statistical summaries of the collected data as well as a brief literature study of the historical state of affairs within the cyber exercise sector. While the focus of this chapter is on the trends of European exercises there is also the overall context of observable global trends.

The final chapters present an analysis of the collected data. It offers both theoretical observations on how and why policies on learning evolve, and empirical observations of practical impacts of, and trends in, the cyber exercise arena.

[2] ENISA Report on National and International Cyber Security Exercises, survey, analysis and recommendations. 2012., https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-exercises/exercise-survey2012

2. Exercise data modelling

Over the last decades, the concept of "New Public Management" (NPM) has slowly gained ground as a means to achieve increased efficiency and effectiveness in government,[3] and while NPM itself has slowly fallen out of favour since the turn of the century, some of its core ideas have made a lasting impression. One of these is that public actors need to be scrutinised and evaluated according to some performance measurement, and have their effort and methodology be adjusted or redirected accordingly to effect a higher level of performance.[4] However, the theory is contingent on the sensible definition of performance metrics, which has proven to be hard in reality to pinpoint. In particular, there is often a rift between what a given institution might see as its core purpose and what the governing body overseeing that institution sets up as metric to be measured and evaluated.

For the cybersecurity area, and relevant to the aims of this report, this might manifest itself as trying to measure vague concepts such as knowledge acquisition or knowledge upkeep in terms of number of training exercises being run.

Exercises present an interesting challenge as an object of study since organising and participating in them is a skill in itself, which improves over time as one attends more exercises. As an actor becomes exercise savvy, their skill level will change what types of exercises the actor can put together and what they can learn from them.

Although we might see that a given actor becomes much better at organising exercises over time (reduced planning time, less disruptions, more detailed or otherwise informed results, etc.), the actual knowledge acquisition suffers, due to a shift of focus from what the exercise tries to achieve (goals) to how the exercise should be perceived (successful project).

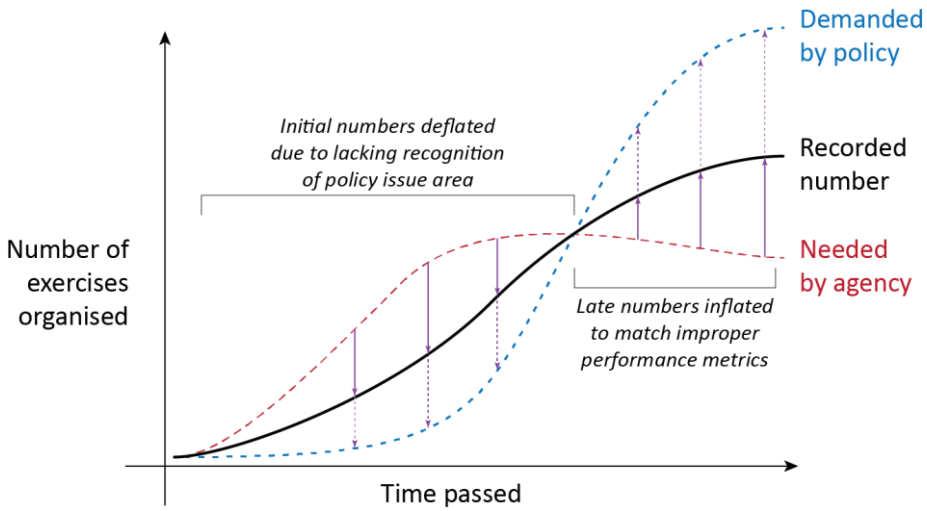

Figure 2: Policy vs. competence pressure

[3] Cf. Klijn, H. E. 2008, "Governance and Governance Networks in Europe", *Public Management Review* 10(4):505-525; Pollitt, C. & Bouckaert, G. 2011 "Comparative Public Management Reform" In Pollitt, C. & Bouckaert, G. 2011, *Public Management Reform: A Comparative Analysis*, Oxford: Oxford University Press, pp. 1-30.

[4] Hood, C. (1991) "A Public Management for all Seasons", *Public Administration* 69:3-19.

A critical part of exercise knowledge is to develop good methods for critical reflection and after-action reports — a part that ties directly into the goal of having as many actors as possible record their activities in the dataset, or indeed to make use of the dataset at all. **Figure 2** is describing the interplay between the demand of policy makers and the actual institutional needs.

2.1 Towards a new metric of exercises

Creating a good historical record of exercises, as well as creating a knowledge repository for previous activities and lessons learned requires an updated method of collecting the relevant data. Somewhat paradoxically, to allow for the development of a good metric, the data set should have enough flexibility, which necessitates the use of highly open-ended questions and categories. While some of the data are quantitative, the dual goal of providing a repository of knowledge and focusing on context and outcomes means that the vast portion of data will be qualitative in nature.

The overall methodology behind this report is similar to the 2012 Cyber Exercises Analysis Report, as this report serves as a continuum. The main difference is that this report has further developed the variables used for the open source scanning process, thus resulting in new findings.

Another key difference in this study is that it attempts to capture the context of the exercise by having a holistic approach that includes not only the participants but the exercise planners and by considering the immediate and long-term planning and outcomes.

It is important to make a distinction between the data being collected and the analytical conclusions that can be drawn from them. For instance, an exercise might be organised in order to acquire new skills, but this purpose will be captured differently depending on who is learning what lesson. Participants acquiring new technical skills is a distinct outcome from exercise planners learning exercise management skills, which in turn is a distinct outcome from everyone improving their skills at introspection and evaluation of lessons learned—that is, becoming exercise savvy. In each case, it is a matter of improvement, but exactly what (and who) is being improved, differs significantly.

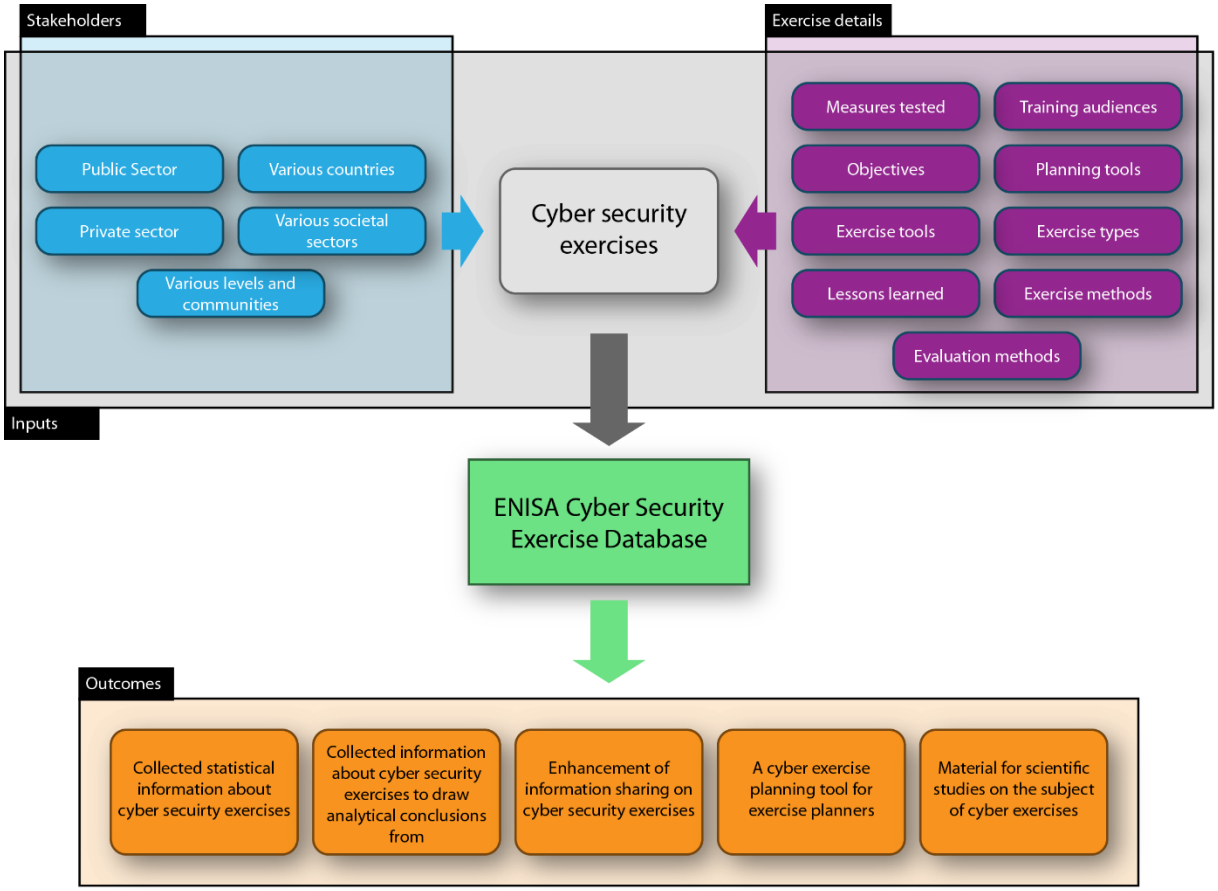

Figure 3: Inputs and outcomes of the study

2.2 Development of the exercise data model

The creation of this repository has followed a four-step process:

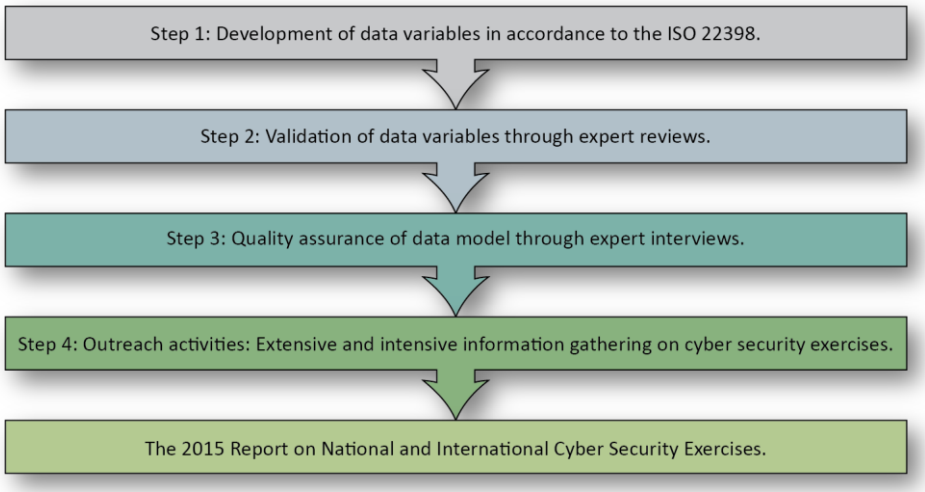

Figure 4: Steps towards launching the exercise dataset

Since terminology and practices concerning exercise methodology and cybersecurity can vary widely, this study's data model variables are based upon the international standard ISO-22398.

Furthermore, a balance had to be struck when formulating variables so as to produce high quality information without jeopardizing the confidentiality and privacy of the scenario or injects. The number of variables also required a balance between providing a full picture of the phases of the exercises and thus valuable information; without threatening the user-friendliness of the results.

The second step consisted of reviewing the variables by consulting a number of experts from a range of different countries and organizations in the cybersecurity exercises community. During this phase, the experts had the opportunity to provide input on which variables were of importance from their perspective.

The third step consisted of quality assurance of the final data variables; this was done by interviewing experts from the field, with knowledge of exercise methodology.

The fourth step consisted of outreach activities. This included extensive information gathering on cybersecurity exercises. One of the outreach activities was open source scanning, gathering data about conducted and planned cybersecurity exercises from all over the world between the years 2013 and 2015. When using the information gathered from open sources, it is important to note that the statistics resulting of open source scanning may not be to a full reflection of the reality. The data gathered via open source scanning are on several occasions only partial, as all desired information regarding certain exercises was not available.

A cyber security survey was also developed using the same variables from open source scanning. The survey includes responses from a network of stakeholders in the global cyber exercises community was included in the report.

2.3 Structure of data model

The data model has four parts. The first part, called "general information" includes fundamental information about the exercise such as name, organiser and objectives of the exercise as well as information about the trained audience. This part provides a basic overview about the exercise and its framework.

The remaining parts reflect the phases of the exercise lifecycle: *planning, execution* and *results* and *improvement*. The planning part entails information regarding planning duration and exercise planning tools. The purpose of this part is to provide an overview over the features of the planning, and to identify common tools used during the planning phase of a cybersecurity exercise.

The execution phase, in turn, entails information such as duration of the exercise, the adopted method as well as the type of exercise. The purpose of the data variables in this phase is to provide an overview of the type of exercise and its methodology.

The final part, refers to the results and improvement phase of an exercise, variables involved include the evaluation method and lessons learned. The purpose of this part of the model is to provide information about the features of the evaluation part of an exercise, as well as the lessons learned from an exercise organisation perspective.

3. Cybersecurity exercises overview

There has been an exponential growth in the number of cyber security exercises over the past decade with the trend expecting to accelerate in the coming years. The pattern of growth up until 2014 was often characterized by a sharp increase from the preceding year followed by a slight decrease. This repetition of peaks is illustrated in **Figure 5**.

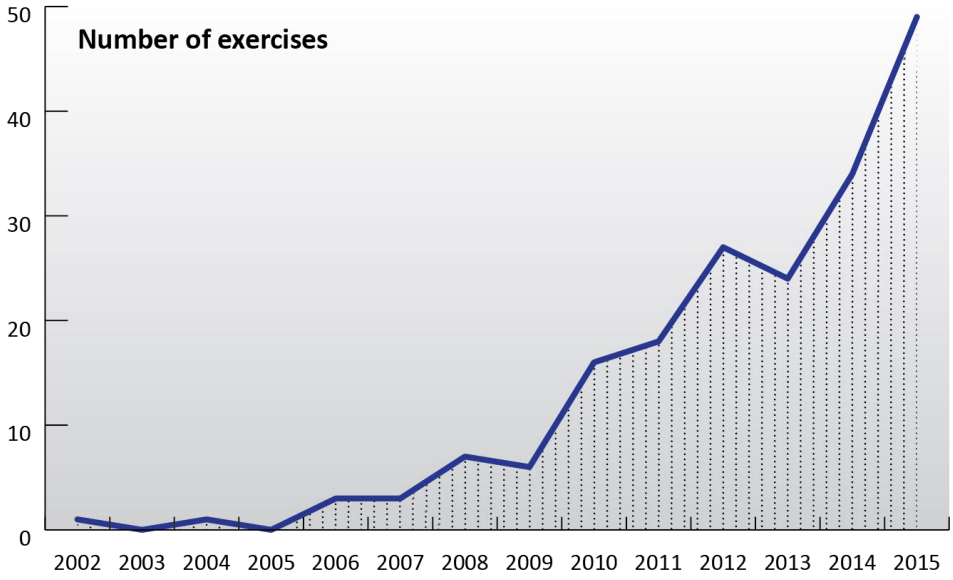

Figure 5: Number of exercises between the years 2002-2015

The data gathered for this report suggests that this pattern is based on the combination of a large number of annual exercises alongside an equivalent large number of biannual exercise series. The pattern is perpetuated as more exercise organisers are added to the mix each year and further reinforced by having more exercises be part of a series rather than one-time events.

3.1 Cybersecurity exercises in Europe

Europe is a major player in the field of cybersecurity exercises. In the last three years, Europe was responsible for over 40% of all global exercises.

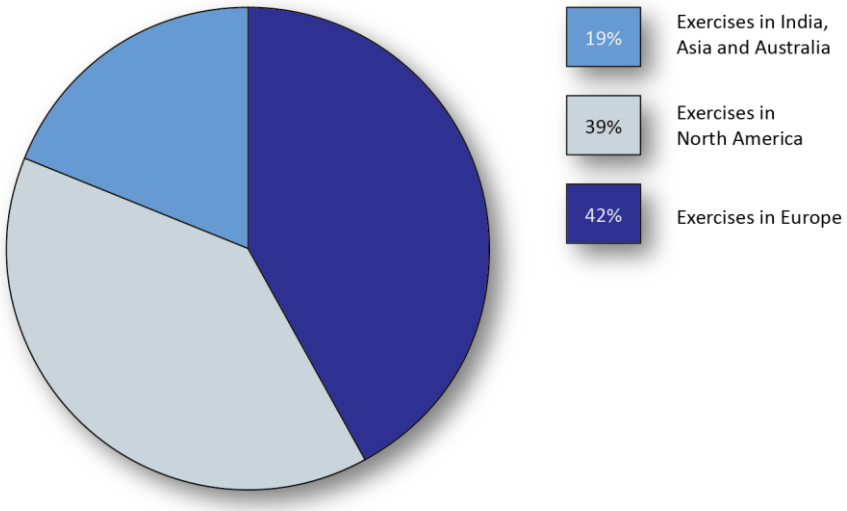

Figure 6: Exercise held in Europe compared to the rest of the world

The number of exercises conducted in Europe during the period of 2012-2015 increases rapidly when compared with these organised during 2013-2015.

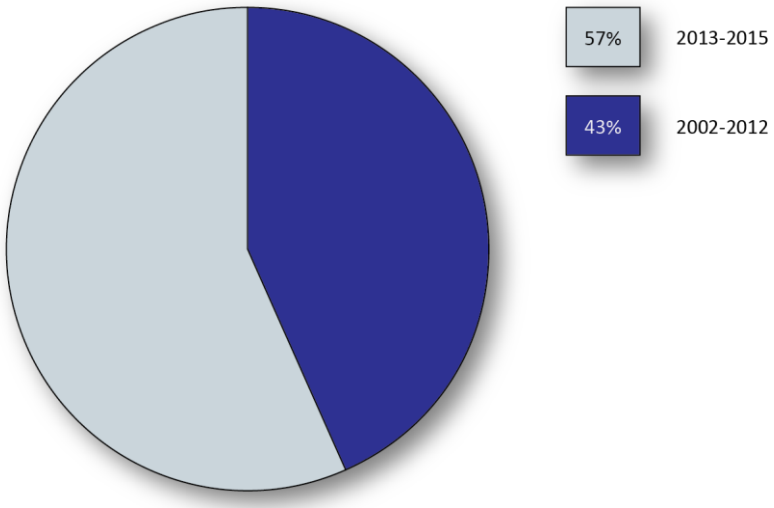

Figure 7: Exercises in Europe over time

The European cybersecurity exercises conducted during the past three years constitute almost two thirds of the total amount of European cybersecurity exercises conducted during the past thirteen years (2012 – 2015).

The rapid increase of cybersecurity exercises in Europe is not only an increase in one-time exercises, but also of regular recurring initiatives in the form of annual or bi-annual series.

As **Figure 8** illustrates, during the past three years almost half of the cybersecurity exercises analysed were one off exercises the other half were part of recurring series. Looking into the past thirteen years, there is a 60%-40% relationship between the two types in favour of exercises conducted as a part of a recurring series.

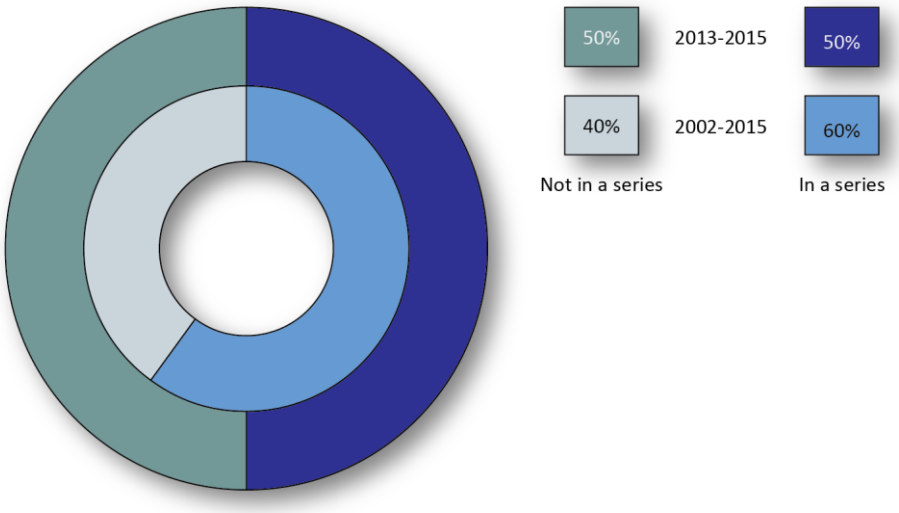

Figure 8: Exercises in a series

3.2 Cybersecurity exercises globally

The exercises in Europe represent over 40% of the global total. North America is an equivalently big actor in cybersecurity exercises as almost 40% of the total number of exercises analysed were conducted there.

Other than Europe and North America, Asia, India and Australia represent around 20% of the overall cybersecurity exercises analysed. An interesting development in Asia is that Malaysia has increased their presence in cybersecurity exercises as they represent 23% of all the cybersecurity exercises conducted during the past three years in the region. Another major actor in Asia is Japan, which either has been a part of or has conducted 26% of the exercises in Asia according to our findings.

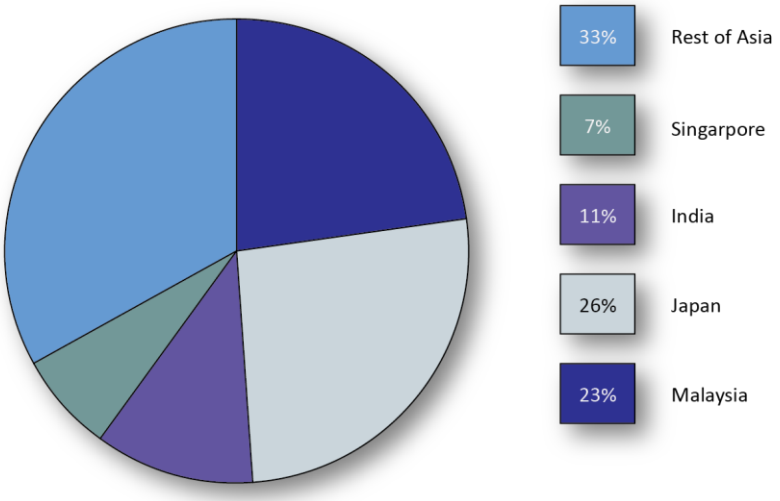

Figure 9: Cyber exercises in Asia, 2013-2015

However, comparing Malaysia to Japan, Japan seems to have a longer history of conducting cybersecurity exercises as they have conducted almost 30% of the cybersecurity exercises in Asia in the period 2002 and 2012, while Malaysia stands for 4% in the same period.

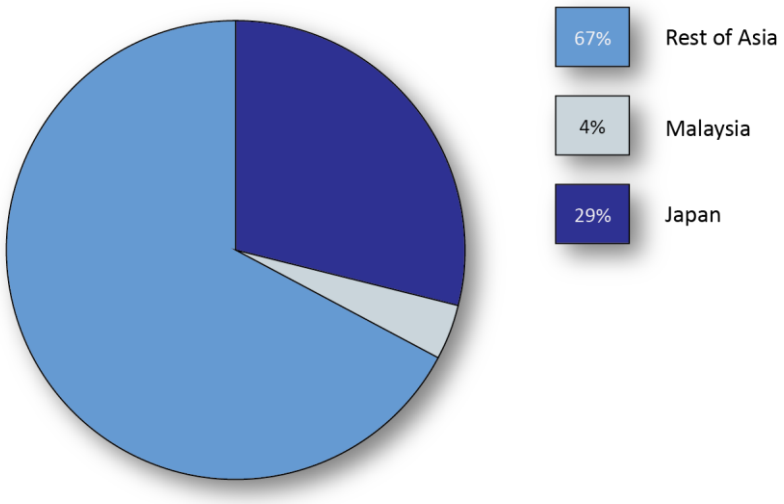

Figure 10: Japan & Malaysia vs. rest of Asia, 2002–2012

In addition to the above, India accounts for 11% of the cybersecurity exercises in the segment and Singapore accounts for 7%.

3.3 Types of cybersecurity exercises

The dataset contains a wide variety of exercise types, as they were described by their organisers, however, based on parameters from the international standard ISO 22398, the set was narrowed down to three main categories based on: a) exercise design, b) performance objectives and c) exercise methodology.

When characterising the exercises using its objectives the following four categories were identified:

1. Develop capabilities
2. Evaluate capabilities of individuals, organisations and systems
3. Measure knowledge, ability, endurance and/or capacity
4. Train the participants and provide an opportunity to gain knowledge, understanding and skills

The empirical data gathered indicates that there is a tendency for most exercises were designed to focus on *training the participants, and provide an opportunity to gain knowledge, understanding and skills*. This particular exercise design represents a 47% of the cybersecurity exercises covered in our analysis, followed by those designed to focus on *developing activities, abilities and ideas* that represents 31% of the exercises covered. The findings suggest that *evaluating the capabilities of individuals, organizations and systems* (14%) as well as *measuring knowledge, ability, endurance and/or capacity* (8%) are not as common as the other two. Considering that, the field of cybersecurity is still relatively young, exercises focusing more on *developing* or *training* are quite understandably more popular.

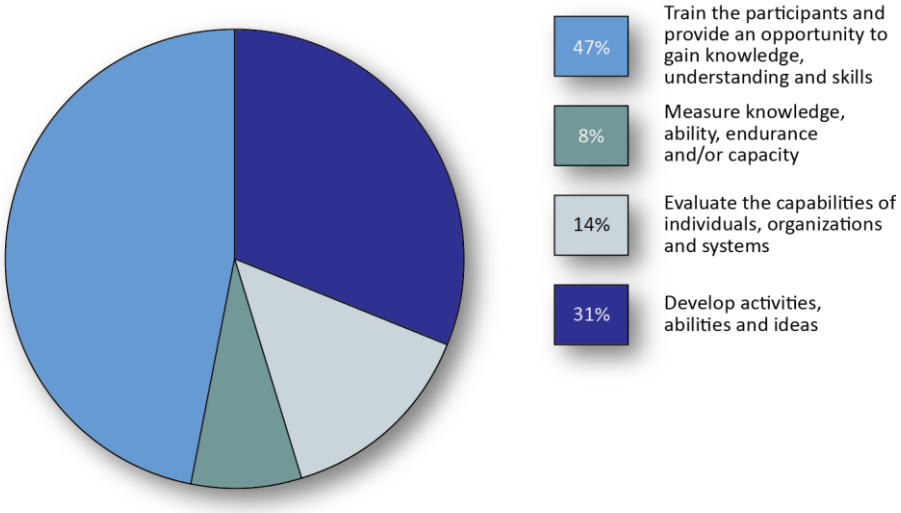

Figure 11: Exercise design

More than half of the cybersecurity exercises covered in the empirical data have a performance objective focusing on *learning*, rather than *cooperation* or *orientation.* The performance objective focusing on *orientation* accounts for 26% of the exercises covered, leaving *cooperation* with 17%. Cooperation exercises are by their very nature more complex as they requires more actors than one organization.

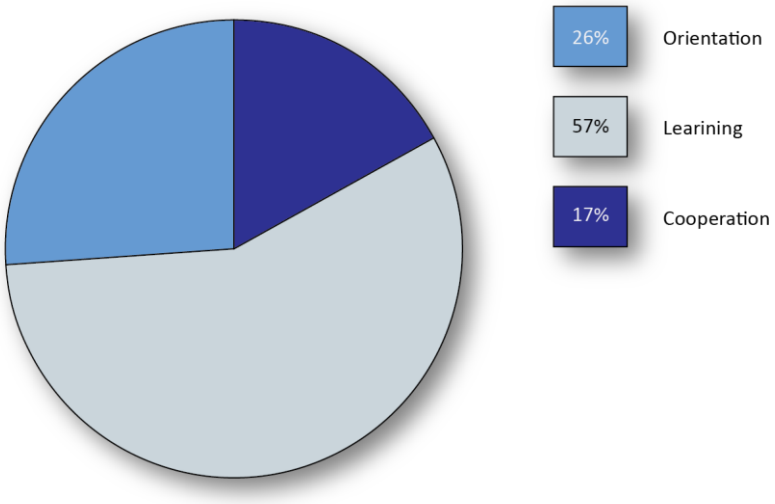

Figure 12: Performance objectives

The findings of the research indicate that the exercises methodology and terminology utilized during the exercises raises challenges depending on the what the methodology actually addressed (skills, process, business continuity) However, based on the international standard ISO-22398 and input from experts, the following types have were singled out :

- Capture the flag
- Discussion based game
- Drill
- Red team / blue team

- Seminar
- Simulation
- Table-top
- Workshop

Most of the exercises analysed were *simulation, table-top* and *workshop*, representing 81% of the total, whilst r*ed team / blue team* represented 11 % of the total exercises collected. Out of the *simulation, table-top* and *workshop* group, *simulation* exercises count for 35%, closely followed by *table-top* at 26% and workshop with 20%.

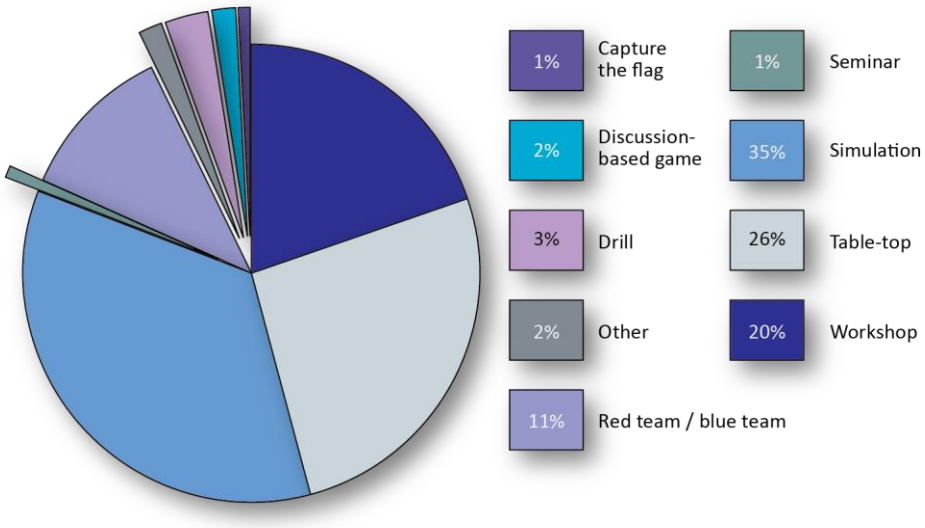

Figure 13: Exercise method

3.4 Cybersecurity exercise practice

There are three main phases[5] in exercises:

1. Planning
2. Execution
3. Evaluation

3.4.1 Planning and conducting

The prominent features of exercise planning and execution, especially concerning complex, large-scale and multinational cybersecurity exercises are the following:

- Most large-scale cybersecurity exercises post 2012 are complex projects. Especially exercises at the national and multinational level, such as Cyber Europe and Cyber Storm IV which involve a large number of participants and a variety of organisations, experts and stakeholders.
- Cybersecurity exercises with strategic level audiences generally require years of planning, and the planning process involves input from diverse stakeholders and experts from participating countries.

[5] ISO 22398

- The empirical data demonstrate that large-scale cybersecurity exercises are commonly managed over an extended period. For example, the Cyber Europe exercise of 2014 had a time-span of one and a half years, and Cyber Storm IV series had a time-span of over two years.[6]
- The planning period is the most time exhausting of the total time-span of an exercise, especially regarding the large-scale multinational and multi-level cybersecurity exercises.

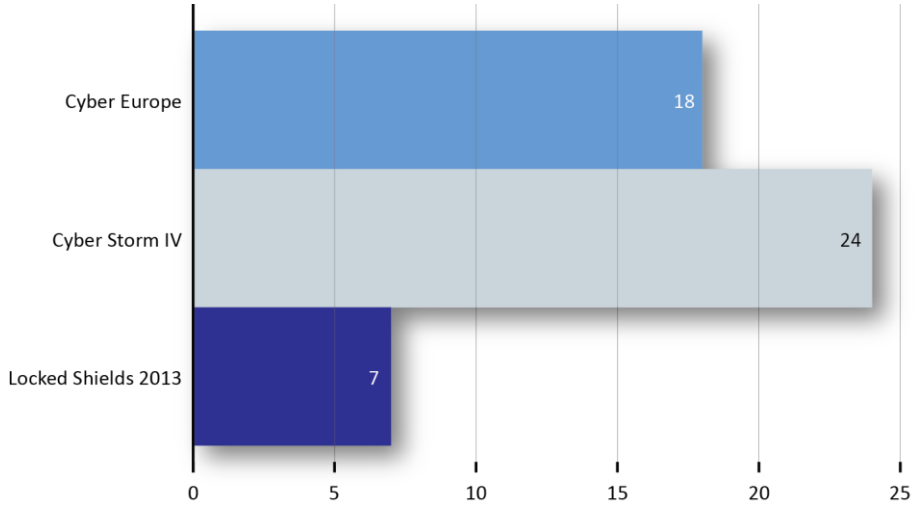

Figure 14: Exercise time-span in months

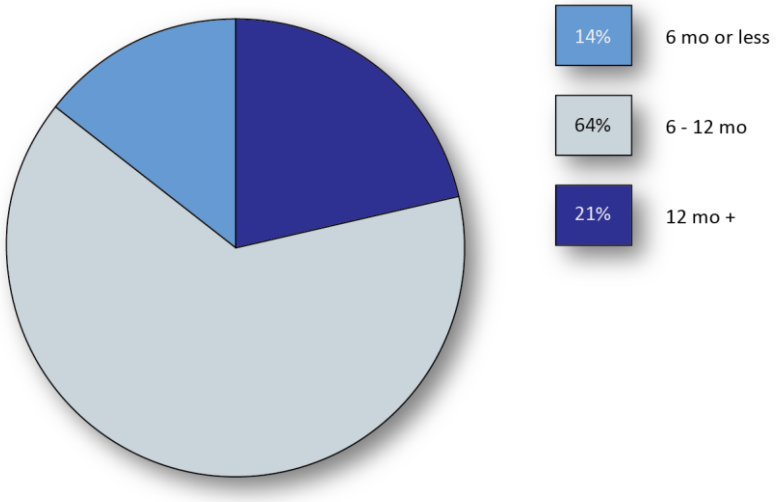

Figure 15: Exercise planning duration

Another prominent feature of these major cybersecurity exercises is that they are divided into a number of sub-exercises and phases, with diverse training audiences and levels in each sub-exercise. For example, one sub-exercise entails domestic public training audience and executing the exercise method table-top, while another sub-exercise entails international training audience and executing the exercise method simulation.[7]

[6] http://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf,
[7] http://www.dhs.gov/cyber-storm-iv

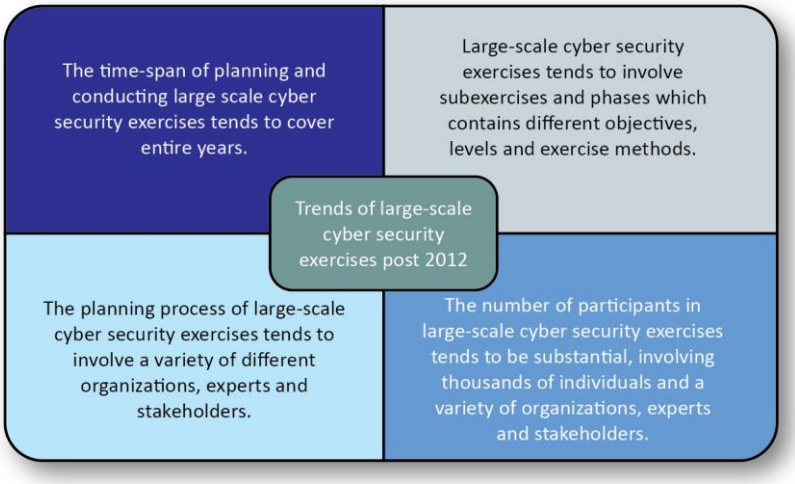

Figure 16: Trends of large-scale cybersecurity exercises post 2012

3.4.2 Exercise evaluation

Evaluation is defined in ISO 22398 as *the systematic process that compares the result of measurement in relation to recognized criteria to determine the discrepancies between intended and actual performance*.[8] During the exercise evaluation phase organisers and participants gather experience from the exercise which transcend to lessons learned.

The empirical data supports the following findings regarding exercise evaluation[9]:

- There is a shift towards not only evaluating if exercise objectives are met, but also evaluating the exercise method in order to gain insight so as to further develop the exercise in the future.
- The evaluation and outcome from for example Cyber Storm IV highlighted important societal developments, such as the need for implementing awareness campaigns.
- Many exercises, especially the large-scale ones, publish "after action reports", reviewing the purpose, scope, planning and execution, scenario and the result as well as lessons learned.
- The increased number of large-scale cyber exercises have caused more stakeholders to communicate and create new relationships.

Lessons learned derive from the observation and evaluation of the exercises. They may be used in order to guide further development of measures in order to improve, for example, cyber crisis or incident management capacity. The empirical data demonstrates a number of common lessons learned from large-scale cybersecurity exercises the past years such as:

- Large-scale cybersecurity exercises that involve many sectors require extensive planning and may become to general (loss of focus on cyber security issues).
- Large-scale exercise might benefit from a small exercise being exercised prior to the main project..[10]

[8] ISO 22398
[9] See http://www.pts.se/upload/Rapporter/Internet/2012/Utvardering-av-Telo-11-PTS-ER-2012-16.pdf and http://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf
[10] idem

- For each new exercise in a series, the number of new participants increases.[11]

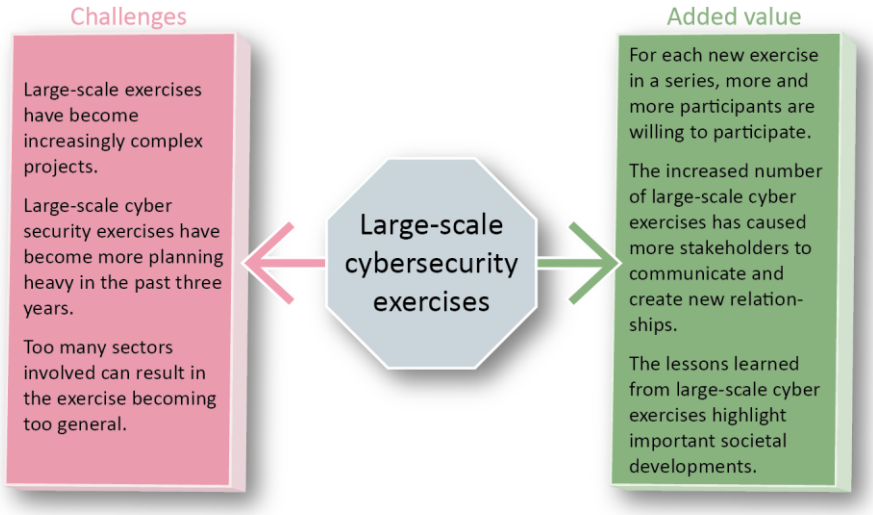

Figure 17: Developments concerning lessons learned

3.5 Trends

Drawing on the information from collected data, four main trends were prominent regarding cybersecurity exercises: increased complexity, cooperation aims, private sector involvement and gap-bridging exercises.

3.5.1 Complexity

Large-scale cybersecurity exercises post 2012 tend to become increasingly complex, often involving a substantial number of participants and a variety of organizations, experts and stakeholders through planning and execution-phases. The total planning-duration time-span of these exercises tends to cover years.

3.5.2 Cooperation

One of the most prominent trends distinguished from the empirical data is the trend of organizing cybersecurity exercises with the aim of enhancing cooperation and coordination of various stakeholders.

The number of cooperation-focused exercises have increased steadily since year 2002. Most interesting is that during the past three years the increase has been over 20% (see **Figure 18**) and the three years before that the number of cooperation exercises more than doubled.

[11] idem

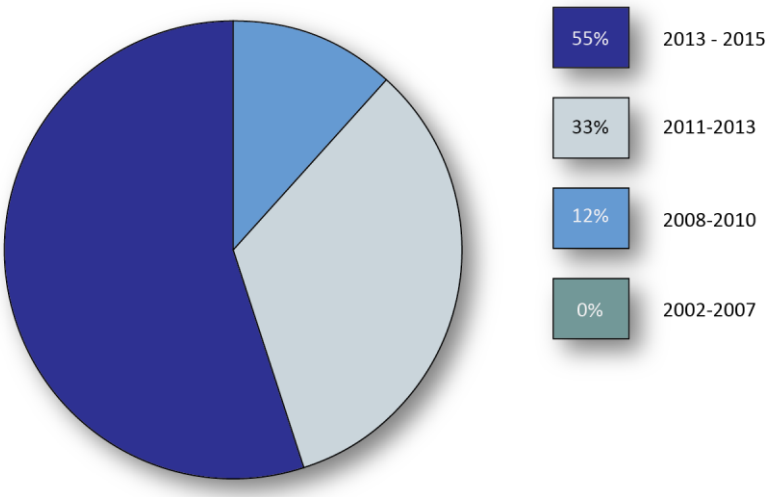

Figure 18: Development of cooperation exercises

Both large- and smaller-scale international exercises covered in the empirical data emphasizes cooperation and coordination as highly important, one of the major focus in an exercise.

For example, the Cyber Coalition 2014 after action report highlighted the importance of exercising communication between various NATO bodies, national cyber defence capabilities, and industry partners.[12] Cyber Europe 2014 provided an opportunity for participants to explore, understand and evaluate EU cooperation mechanisms as well as engage in cooperation at national and European levels.

The after action reports from these and other exercises demonstrate a number of central motivations behind the cooperation objectives[13] as they:

- Allow practice and development of information sharing between involved parties.
- Allow participating parties to tap into each other's expertise, enabling them to achieve greater alignment.
- Enhance shared situational awareness between involved parties.
- Enhance coordination between involved parties.
- Advance public-private partnerships.

3.5.3 Private sector involvement

Besides emphasizing the importance of cooperation between various stakeholders, the empirical data we have gathered demonstrate the emerging trend of involving both private and public sectors in cooperative exercises. It is important to note that the limitation of our dataset should be taken in to account, since the research was not exhaustive. Private companies may very well focus more on their internal process and procedures which could not be captured in the dataset. Nevertheless, our data suggests that there are strong initiative in the area of public-private cooperation.

[12] https://www.ncia.nato.int/NewsRoom/Pages/141126-cyber-coalition.aspx
[13] http://www.eurofibergroup.com/media/latest-news/59/cyberdawn-exercise-tests-security-cooperation-in-telecom-sector

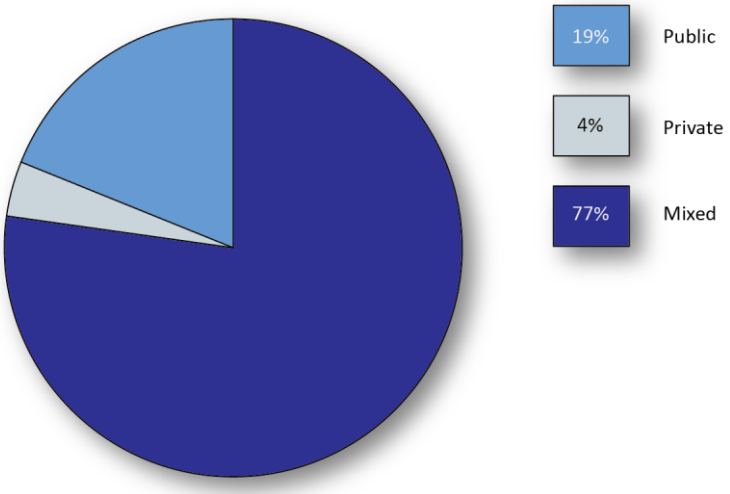

Figure 19: Sector involvement

For example, one of the Cyber Europe 2014 objectives included exploring the cooperation between private-public and private-private players.[14] Cyber Storm IV objectives aimed at enhancing the advancement of private-public partnerships within the critical infrastructure sectors,[15] and one of the objectives of the 2013 Cyber Attack & Business Continuity simulation included examination and demonstration of private sector and public sector (government) information sharing prior to, during and following an act of cyber terrorism. Moreover, one of the outcomes from exercise Cyber Guard 2015 was the importance of synergy with the private sector partnerships.[16]

The after action reports from these and other exercises, national cybersecurity strategies from numerous countries as well as international reports such as the ENISA Report on Cyber Crisis Cooperation and Management reveal the key motivations behind the private sector involvement:

- Cross-border cyber risk and threat-landscape requires information sharing and collaborative efforts between private and public bodies.[17]
- Private and public cybersecurity partnerships face challenges due to divergence of standards, communication and terminology.[18] Involving private and public actors in cybersecurity exercises supports bridging of this gap.[19]
- Involving both private and public sectors in the same exercise supports shared awareness.[20]
- Involving both private and public sectors in the same exercise supports further development of their respective capabilities as well as their capacity to act collectively.[21]

[14] Cyber Europe: An overview
[15] http://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf
[16] http://www.defense.gov/News-Article-View/Article/604934
[17] Report on Cyber Crisis Cooperation and Management P. 41, http://www.defense.gov/News-Article-View/Article/604934,
[18] Report on Cyber Crisis Cooperation and Management P. 41 & p. 30
[19] http://www.defense.gov/News-Article-View/Article/604934
[20] Cyber Europe 2014: After Action Report
[21] http://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf

3.5.4 Gap-bridging exercises

The current threat-landscape requires the contribution of different stakeholders from various levels and with diverse expertise to cooperate. Some of these stakeholders may not collaborate nor even communicate with each other on a regular basis, which generates gaps and becomes an obstacle for efficient cybersecurity collaboration. One of the prominent trends of this report is the use of cybersecurity exercises as a gap-bridging measure.

The post 2012 exercises included scenarios that aim at bridging the cooperation gaps between various actors. Moreover, exercises aim at bridging the gap between for example operational and strategic levels, between decision-makers and the technical levels, or between policy makers, operational management and the technical staff have become apparent in the post 2012 empirical data.

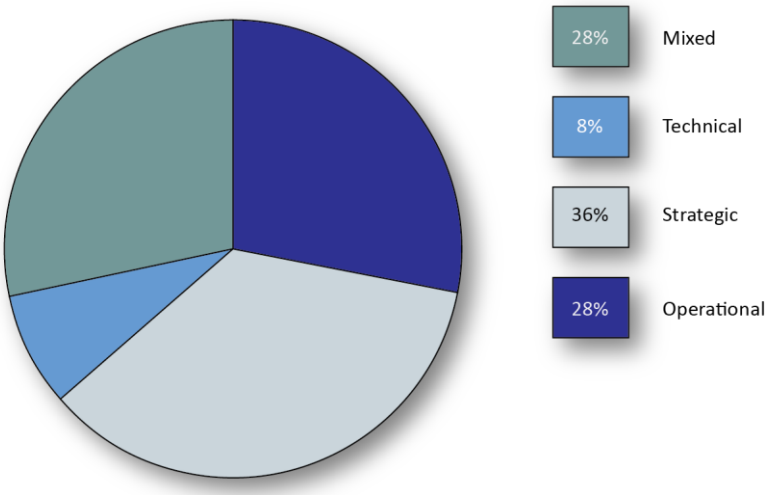

Figure 20: Exercise level

Exercises focused on strategic level issues still represent the majority, however, closely followed by mixed level exercises and bridging the gap between the various levels. This supports the findings and recommendations presented in the Report on Cyber Crisis Cooperation and Management, which discusses the increased need for mixed level exercises in order to strengthen the communication between technical and non-technical levels.[22]

[22] Report on Cyber Crisis Cooperation and Management P. 46

4. Analysis

4.1 Growth of Cybersecurity exercises

There are several reasons behind the growth of cybersecurity exercises. Arguably, the prominent reasons derive from a general increase of awareness regarding cybersecurity issues and the importance of cybersecurity exercises, created by various activities at national and international levels.

4.1.1 The impact of national and international cybersecurity strategies, trend reports and publications

The increasing number of EU-countries (and outside the EU) implementing national cybersecurity strategies has supported the increased awareness. The national cybersecurity strategies commonly stipulate the countries actions, planned actions and objectives towards enhanced national capacity regarding cybersecurity management. A feature of these strategies is their emphasis on the importance of participating in (and sometimes organizing) cybersecurity exercises, both domestic and internationally.[23]

Likewise, the Cybersecurity Strategy of the EU (2013) has also contributed to improving awareness, by outlining strategic priorities and actions for enhancing cybersecurity both nationally and for the EU collectively. Additionally, the strategy was accompanied by a proposal for a Directive in Network and Information Security (NIS Directive), aiming to "ensure a high common level of network and information security and require Member States to increase their preparedness and improve their cooperation".[24] The Cybersecurity strategy of the EU also emphasize the importance of pan-European cybersecurity exercises, and describes them as essential to stimulate cooperation among the member states and the private sector. Moreover, supporting EU-wide cybersecurity preparedness exercises is one of the main actions of the Digital Agenda for Europe, the new policy plan of the European Commission.

ENISA has continuously contributed to the increased awareness by (along with other activities) publishing international reports and studies. During 2013, ENISA released the report "Cybersecurity cooperation – defending the digital frontline", aiming to assist the EU member states in attaining increasingly higher levels of cybersecurity preparedness. The report highlighted the need of cross-border collaboration, cyber incident reporting in the EU, as well as cyber crisis cooperation and exercises.[25] The following year ENISA released another publication "Report on Cyber Crisis Cooperation and Management" which aimed to provide an analysis of the emerging field cyber crisis management in relation to general crisis management. In order to deal with the cyber crisis management challenges identified in the study, one of the main recommendations included further training and exercise activities – inter-sectorial and cross-sectorial, national and international and involving both public and private actors.[26]

4.1.2 Important incidents and reports on cyber threats

During the recent years, both incidents and reports on cyber-threats has served as "wake-up calls" and raised awareness of cybersecurity issues. Cybersecurity incidents such as Estonia 2007, where some of the Estonian government online services (including online banking) became disrupted, and STUXNET – a

[23] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/national-cyber-security-strategies-ncsss, Cyber security strategy of the Netherlands 1 & 2, Cyber security strategy of Finland, Cyber security strategy of the EU, p.3
[24] Cyber security cooperation - Defending the digital frontline - October 2013 p. 8
[25] idem pp. 12-16
[26] Report on Cyber Crisis Cooperation and Management Comparative study on the cyber crisis management and the general crisis management P. 4-5

sophisticated malicious code discovered 2009, which disrupted the Iranian uranium enrichment centrifuges, served as major "eye openers" for many cyber dependent countries. [27] More recently, the advanced malware "Snake", which infiltrated government and military organizations of several countries, was discovered 2014.

Reports on the current and emerging cyber threats such as the ENISA "Threat landscape 2014 – overview of current and emerging cyber threats", and the "Cyber Security's Infamous Five of 2014" has continued to emphasize the increasing complexity of attacks and the successful attacks on vital security functions of the internet. [28] The reports highlight that the cyber-threat landscape is changing, and that the number and scope of major cyber breaches continue to increase.[29]

4.1.3 The compound growth of Cybersecurity exercises

The growth in the number of cybersecurity exercises are compounded by the need to follow up on the results and lessons learned of the previous exercises thus generating more exercises. For example, In order to continue the improvement of preparedness and improved response capabilities it is necessary to have further training and education through seminars and exercises.[30]

Indeed, experience and lessons learned from conducting exercises illustrates that participation in cybersecurity exercises works advantageously for cybersecurity capacity in a number of ways:

1. Assess and test capability, organization and methods, and the results may provide a knowledge base on which further progress of capacity building actions may be developed.
2. Enhance coordination and collaboration between participating parties.
3. Provide an opportunity of sharing knowledge between participating parties.
4. Enhance awareness and skills, both individually as well as collectively.
5. Support the establishment of cooperative mechanisms.

4.2 Cybersecurity exercises in an exploratory phase

This study highlights cybersecurity exercise trends such as increasing complexity, cooperation aims, private sector involvement and gap-bridging exercises. Especially large-scale cybersecurity exercises tend to include increasing amounts of actors and stakeholders. There are good reasons for involving different types of stakeholders in the same exercise and aim for new cooperative relationships of actors to be established.

For example, the cross-border nature of cyber risks and threats, the need for collaborative efforts when managing cyber-incidents and the positive impact which cooperative exercises has on establishing cybersecurity collaboration has made involvement of the private sector in large-scale cybersecurity exercises essential.

However, there is a risk in constantly adding new elements, actors and cooperative structures; since many contemporary cybersecurity exercises tend to focus on exploration of new factors rather than consolidating on the already established capabilities, procedures, mechanisms and information flows. This development implies that that cybersecurity exercises generally are still in an "exploration phase", which is reflected in their objectives.

For example, the objectives of large-scale cybersecurity exercises such as Cyber Coalition, Cyber Europe and Cyber Dawn, conducted during recent years, emphasize the exploration of cooperation and cooperative

[27] http://www.reuters.com/article/2012/02/14/us-iran-usa-stuxnet-idUSTRE81D24Q20120214
[28] ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats, p. 3
[29] Report: Cyber Security's Infamous Five of 2014 – CyActive, p.1
[30] http://www.dhs.gov/sites/default/files/publications/Lessons%20Learned%20from%20Cyber%20Storm%20IV.pdf

mechanisms between the various stakeholders involved. Moreover, many large-scale exercises emphasize learning and training of the involved stakeholders, aiming to make the exercise audience more comfortable with newly introduced structures.

A challenging consequence of adding new elements, actors and cooperative structures to every new exercise is that the capabilities, procedures, mechanisms and information flows explored in one exercise, change in the next one. Therefore, due to the new added elements, the exercise yet again becomes explorative instead of consolidating and quality improving by building on the experience from procedures, mechanisms and information flows explored in the previous exercise. For exercise planners in exercise series, improvement of for example methodology and coordination may also pose a greater challenge when every new exercise entails several new elements and actors, which leads to further complexity challenges.

Exploring new cybersecurity structures and collaborations in exercises is undoubtingly an important step towards consolidation. However, exploring the structures and collaborations will not solely generate established capabilities, procedures, mechanisms and information flows – especially not when these are highly complex and transcend both geographical and sectorial borders. This would instead require exercises with the focus on establishing and consolidating already explored structures and collaborations.

4.3 Cybersecurity exercise outcomes and challenges

Exploration is a defining characteristic of exercises. Even an exercise that fails to fully meet its objectives may still be highly instructive to both planners and participants in terms of the capability and identified knowledge gaps. Conversely, an exercise may fulfil every criterion for success as set up by the planners, but may nevertheless be of doubtful value to the knowledge acquisition or retention of the participants.

In the policy related bibliography, there is the phenomenon called “fantasy documents”[31]. This term refers to policies and plans which set in response to an event without any real concern for whether or not they are fit for purpose. Rather, they are purely symbolical relics of a political need, mainly the need to be seen as taking some kind of action to rectify or address previous mistakes and assumed needs. While at first glance, this phenomenon may be read as policy failure, it is more often than not just the inherent result of a modern form of governance that assigns an elevated value to planning and checklists. It is a belief that the *plan itself is* the actual solution, rather than the eventual execution of that plan should a problem (re-)emerge.

Secondly, the literature suggests that after-action reports and “lessons learned”-documents have become increasingly at risk of becoming fantasy documents.[32] There is an increased demand that lessons *must have* been successfully learned, and that noting such instances of lesson-drawing is all there is to it. Few, if any, controls are actually made to verify that they can even be called lessons by any sensible definition, or that anything has actually been learned. Quite the opposite: there is even an observed tendency to *over-learn*; to not actually take stock of what works and what does not, and especially not of why this was the case, but rather to assume that if something went wrong, a complete overhaul and restructuring is required. After all, if something went wrong, then obviously the processes were not good enough? It is an instinctive but highly dangerous assumption to make—sometimes, circumstances conspire to make success impossible, and even the best-laid plans come to naught. This is if anything a far more important lesson to learn than most: that

[31] Cf. Clarke, L. 1999, *Mission Improbable*, Chicago, IL: Chicago University Press; Birkland, T. 2006, *Lessons of Disaster*, Washington, D.C.: Georgetown University Press; May, P. 1992, “Policy Learning and Failure”, *Journal of Public Policy* 12(4):331–354.
[32] Birkland T. 2006.

everything was handled above and beyond what could be expected, but the outcome was all but inevitable anyway, so while it may be a hard sell, the best way forward is to change nothing.

The early data suggests that attention *is* being paid to this area. There is an increased focus on *process evaluation* to parallel the regular measuring of objectives, as well as a nascent awareness that an informed and focused selection of participants might yield better results than all-encompassing mega-exercises. That is not to say that cross-sector or gap-bridging exercises should be avoided — quite the opposite — but rather that no value is added in increasing the participant count of an exercise just for the sake of making it large and spectacular.

At the same time, the value of a good spectacle should not be underestimated. Aside from testing or improving knowledge among participants, an important role that such exercises play is to raise awareness of cybersecurity issues and the numerous social and technical complexities that they create. It is a debate for a different time and place whether such awareness-raising is best done through actual participation in exercises or whether mere observation is enough, but the raised awareness of the issues an exercise is meant to explore is still an important outcome that needs to be taken into account during the planning phase. While such measures may often be *aimed at* a policy level, for instance to demonstrate the need for adjusted metrics or focus areas as suggested in previous sections, the success of this type of communication should be very high on the planners' agendas since it may very well determine the viability and scope of future exercises. Once again, it is worth remembering that a single exercise can have many different purposes, each depending on the particular audience. This type of communication and education of decision-makers may end up being a very decisive factor in effecting policy changes that improve the capacity and capability of the cybersecurity sector as a whole.

A closely related outcome is the promotion of the exercise itself. Collaborative and increasingly complex exercise designs are on an upwards trend, and attracting new expertise and new participants is a crucial part in continuing this trend. There is nothing inherently negative about this trend that would suggest that it should be combatted or reversed. Rather, the question is how best to find the right audience for this type of promotion. The dataset designed in conjunction with this study is one tool for doing so, but relies on self-selection on the recipient's end: a process of them looking for ideas that might suit their needs and finding previous examples in the dataset.

In the data collected, there are the occasional examples of this type of outreach, but it highlights that there are two rather separate interpretations of this outcome. One is where new participants find out about and seek to join an existing exercise; another is what might almost be seen as a franchise model, where organisers offer exercise designs—either as loose templates or as entire ready-made packages—that other interested parties might pick up and run on their own, more or less tweaked to their own specifications. If the trend towards a more reflective and process-analytical approach to post-exercise learning continues, the best practices spawned from such reflections will no doubt create yet another knowledge that needs to be promoted in the cybersecurity sector.

5. Conclusions

This study is based on consisting sample of over 200 exercises globally, which means it is not exhaustive but quite inclusive. The dataset presents a good overview of the developments between the years 2012 and 2015. Besides the dataset, literature such as after-action reports and previous studies have contributed to the findings and the analysis.

There are several conclusions in this report, many of them in-line with the 2012 Analysis report, such as: there is a continuous increase of cybersecurity exercises, cooperation exercises, national and multination cybersecurity exercises and public-private sector collaboration.

In addition, there is a sharp increase in the total number of exercises held post year 2012. The number of cooperation exercises is also increasing together with the efforts of involving private actors in the cooperation exercises. Large-scale exercises have played an important role in the development of the cybersecurity exercise community from several perspectives, such as private sector involvement but also from a gap-bridging perspective, by mixing technical aspects with non-technical aspects in an exercise.

This report has identified three main reasons that led to this increase. First being the increase of policy and strategy documents that supports cybersecurity exercise activity, such as national cybersecurity strategies, publications from ENISA but also the upcoming NIS Directive. Further reasons behind the increased cybersecurity exercise activity is the real-life incidents and the increased attention that it has generated. Lastly, exercises generate more exercises, especially large-scale exercises such as Cyber Europe that in some cases worked as a door opener to cybersecurity exercise activity.

More cybersecurity exercises focus on exploring new structures and collaboration. Even though these are important aspects in order to reach consolidation, there might be in the best interest of the participants to actually take the next step and start focusing on establishing procedures, mechanisms and so on for collaboration. Meaning that it could prove beneficial to shift the focus towards conducting exercises with the objective of establishing already explored structures.

At the same time, there are a number of potential pitfalls to such rapid expansion that need to be understood and taken into account, and which are of particular importance since we are dealing with exercises—that is, a method for learning.

In the haste to always do more, larger, better, the actual and practical value of the learning that is supposed to take place is left untested and the conclusions unchallenged. Thankfully, introspection is already part of the exploratory phase cybersecurity exercises are currently situated in, but going forward, more attention is still needed in this area. In particular, if the previously mentioned shift towards quality over quantity is to have positive effects, the metrics for what constitutes a “good” or “appropriate” exercise need to be honed.

Finally, the communicative aspects of exercising are still left fairly unexplored in much of the exercise design and planning. While there are undoubtedly links between an increased awareness of cybersecurity issues and an increased number of exercises, the exact nature and scope of the issue area remains a highly technical piece of knowledge, and yet it needs to reach an increasingly large audience—both decision-makers and the public in general. Irrespective of whether it raises awareness of the problems and solutions that different actors in the sector know about, or simply acts as method to promote wider participation and more exercises, almost every exercise is an opportunity to further educate and inform the larger community, but this opportunity is still all too often missed.

6. Recommendations

These recommendations are based on the findings from the analysis of the data collected and of the guidelines established in the 2012 Analysis report. The overall objective with the recommendations is to increase the quality of cybersecurity exercises and enhance cybersecurity resilience.

ENISA should establish a common ground for best-practice exchange regarding cybersecurity exercise

The dataset developed in parallel to this analysis report has the potential to become a common ground for information and knowledge sharing regarding cyber exercises. The dataset should be further developed with a user-oriented interface, promoting that stakeholders themselves are to sustain the dataset by contributing experience, knowledge and lessons learned from their exercise activities. The end goal is that the common ground becomes wide-spread and the "go-to" for knowledge regarding exercise planning and best-practices. This is one of the steps towards establishing a more integrated cybersecurity exercise community, whereas there can be developments regarding methodologies and tools for exercises. *ENISA will lead and complete this work in the near future and assist actors to contribute to the dataset.*

Member States should contribute to the development of cybersecurity exercises community

In order for the ENISA Cyber Security Exercises Dataset to be a source of valuable information regarding exercises, best practices and methodology, it requires input from the community. The greater amount of input from stakeholders involved with exercise activity within the field, it opens up the possibility of using the dataset as a resource for planning and collaboration between nations and agencies, allowing for more efficient and effective training of cybersecurity professionals and decision-makers. This will furthermore contribute to the end goal of increasing cooperation and knowledge sharing within the field. *We recommend all actors involved in exercise activity should contribute to the ENISA Cyber Security Exercise Dataset by providing input during the planning and the evaluation phase in future exercises. This recommendation should be completed in the near future.*

ENISA should analyse cyber exercise trends on a regular basis

The 2012 and the 2015 Analysis report teaches us a lot about the developments within the field of cybersecurity exercises and what the trends have been and what the trends are moving towards. By making this Analysis report a bi-annual publication, it allows for further knowledge spreading, but also, better follow-up on what the impacts are from the developments within the field. The more Analysis reports being drafted, qualitative the analysis can be. Parallel to the bi-annual Analysis reports, the dataset should be revisited and updated according to feedback from the community, contributing to making the ENISA Cyber Security Exercises Dataset as good as possible for the community. *Medium term, ENISA should aim at making the Analysis report a bi-annual publication and that the dataset is reviewed in parallel to the every new Analysis report and updated in accordance with input from the community.*

Member States and ENISA should work towards developing a European exercise calendar

In regards to the increased amount of cybersecurity exercises that are being held in Europe, there is benefit of developing a European wide exercise calendar. The exercise calendar would help in visualising the exercises being held and would increase awareness amongst the actors in Europe. The exercise calendar could be available in connection to the ENISA Cyber Security Dataset, contributing the overall end goal of a widespread cybersecurity exercises community. *As of 2016, ENISA should maintain the exercise calendar and attaches it to the dataset.*

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 Vass. Sofias & Meg. Alexandrou
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

ISBN: 978-92-9204-158-8
DOI: 10.2824/627469