enisa
European Network and Information Security Agency

On National and International Cyber Security Exercises

Survey, Analysis and Recommendations

October 2012

Acknowledgements

ENISA wishes to thank all persons and organisations which have contributed to this stocktaking exercise. In particular, our gratitude goes to the following contributors:

- The cyber exercise community who filled in the online survey published on the ENISA website and provided additional information about the exercises;
- Speakers and participants who attended ENISA's 1st International Conference on Cyber Crisis Cooperation: Cyber Exercises, 27 June 2012, in Paris.

About ENISA

The European Network and Information Security Agency (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.

Follow us on Facebook Twitter LinkedIn Youtube & RSS feeds

ENISA project team

Panagiotis TRIMINTZIOS, Resilience and CIIP Unit, ENISA
Razvan GAVRILA, Resilience and CIIP Unit, ENISA

Contact details

For questions related to this report or any other general inquiries about the resilience program please use the following contact address: resilience at enisa.europa.eu

Executive Summary

Cyber exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. ENISA supports the stakeholders involved in EU cyber exercises.

This report aims to support European and international bodies involved in cyber exercises with lessons learned about cyber exercises and recommendations for the future. The report presents the results of the ENISA 2012 research and analysis by ENISA in 2012 of national and international cyber exercises carried out.

ENISA examined 85 exercises covering the period between 2002 and 2012. In total, 84 countries worldwide participated in the multinational exercises analysed in this report. A total of 22 European countries conducted in national cyber-exercises.

The main findings in this research include:

1. The number of cyber exercises has increased in recent years (71% took place in between 2010-2012). The reasons for this increase are the overall policy context that supports and boosts cyber exercises, the increased emphasis given by the EU Member States to cyber exercises, and the increasing threat of (cross-border) cyber incidents and attacks.
2. Cyber crisis cross border cooperation efforts are continuously developing. Cyber security is an urgent matter which receives increasingly more attention in European countries.
3. Public–private partnerships during cyber exercises are essential due to private sector ownership of most critical information infrastructures. There is a need to intensify public–private cooperation in cyber exercises.
4. More attention should be paid to developing exercise management tools which can support exercise execution and preparation.
5. The use of methodological planning, monitoring and evaluation is crucial for effective exercises.
6. There is broad consensus that cyber exercises help to enhance the preparedness, responsiveness and knowledge of stakeholders in responding to cyber incidents.

The report concludes with seven recommendations for stakeholders in the global cyber exercises area, which aim to increase the number and quality of cyber exercises. The main recommendations are:

1. Establish a more integrated global cyber exercise community;
2. Ensure the exchange of good practices on cyber exercises, including public–private cooperation;
3. Support the development of exercise management tools to support exercise planning, execution and evaluation;
4. Aim for more complex cyber exercises on an inter-sectoral, international and European level;
5. Enhance preparedness by including exercises in the lifecycle of Cyber Crisis Contingency Plans;
6. Update the good practices for national exercises and initiate a good practice guide for multinational exercises;
7. Develop feedback mechanisms for ensuring that lessons learned from cyber exercises are implemented resulting in enhanced cyber crisis preparation.

Contents

List of figures

1 Introduction

Cyber[1] exercises are an important tool to assess the preparedness of a community against cyber crises, technology failures and critical information infrastructure incidents. Exercises enable the competent authorities to target specific weaknesses, increase cooperation across the critical information infrastructure sector, identify interdependencies, stimulate improvements in continuity planning, and generate a culture of cooperative effort to boost resilience in the cyber crisis cooperation area.

In 2009 ENISA issued a recommendation about the importance of cyber exercises. Since then ENISA has continued to support the stakeholders involved in cyber exercises in Europe. This stocktaking report is one of ENISA's efforts to enhance this area in Europe. This report aims to support the European and international cyber exercises community with lessons about cyber exercises and recommendations for the future. The report presents the results of the stocktaking of national and international cyber exercises carried out by ENISA in 2012.

More information about this report, the stocktaking activities and supporting material can be found on the report's companion website at ENISA's Resilience and CIIP public web pages.[2]

1.1 Policy context

In its 2009 Communication on Critical Information Infrastructure Protection COM(2009)-149[3], the European Commission invited Member States to 'organise regular exercises for large scale network security incident response and disaster recovery'. The Tallinn Ministerial Conference, which took place in 2009, subsequently built on the five pillars of the CIIP Action Plan, stressing that 'A joint EU exercise on Critical Information Infrastructure Protection should be organised and staged by 2010, in line with the Commission's action plan'.

As an ultimate confirmation of the importance of exercising at both the national and pan-European level, the Council Resolution published in December 2009 stated that 'Member States should organise national exercises and/or participate in regular European exercises in the area of Network and Information Security'. ENISA fulfils a significant role in this by supporting Member States in providing appropriate responses to emergencies.

Supporting EU-wide cyber security preparedness exercises is one of the main items on the Digital Agenda for Europe COM(2010),[4] the new policy plan of the European Commission which emphasises the need for Member States to carry out large-scale attack simulations and test mitigation strategies in cooperation with the Commission. Here, ENISA's newly proposed mandate again highlights the significance of cyber security preparedness exercises in enhancing trust and confidence in online services across Europe, as well as the exchange of good practices in this area.

---

[1] *In this report we use the terms 'Cyber' and 'Critical Information Infrastructures' synonymously and interchangeably, based on the definition of the former as: ' "cyber" refers to the interdependent network of information technology infrastructures, and includes technologies such as the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries.' (Source: WEF, Partnering for Cyber Resilience, World Economic Forum Report, 2012 available at: http://www.weforum.org/issues/partnering-cyber-resilience-pcr)*

[2] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercise-stocktaking*

[3] *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm*

[4] *http://ec.europa.eu/digital-agenda/*

In this policy context the first pan-European exercise on Critical Information Infrastructure Protection (CIIP), *Cyber Europe 2010*, was conducted on 4 November 2010.[5] The exercise was organised by EU Member States and facilitated by ENISA. Built on a scenario concerning internet resilience, the exercise helped to increase trust and test the communication efficiency between the participating Member States of the European Union and the European Free Trade Association (EFTA), hence illustrating the value of conducting such exercises.

A COM Communication of March 2011, COM(2011)-163[6], on CIIP again stressed the importance of cyber exercises for a coherent strategy for cyber incident contingency planning and recovery at both national and European level. There is therefore an increasing appreciation of exercises as a means of validating CIIP resilience and improving stakeholder communication. As such, the cycle, which began with the *Good Practice Guide on National Cyber Exercises*,[7] is now in full motion after the completion of the first joint EU–US CIIP Exercise, Cyber Atlantic 2011, and of the second pan-European cyber exercise Cyber Europe 2012[8].

1.2 Scope and audience

This report aims to provide a global overview of cyber exercises, analyse their commonalities and differences and finally draw a number of recommendations that could help improve their impact and quality.

In this research we explore the field of cyber exercises, focusing on the way exercises are executed. Our research included information about cyber exercises conducted since 2002 (and about those planned in the near future). Such exercises took place at different levels, such as the national or multinational level and in the private, public or combined sectors.

The target audience for this report consists of stakeholders, policymakers and experts in the field of national, European and global cyber crisis cooperation, and especially those with a responsibility for organising cyber exercises.

1.3 Methodology

As a first step to prepare this research, we conducted a bibliographical search over six months (February–July 2012) in order to gather information on cyber exercises from online sources and available relevant literature.

The second step was to develop a survey about cyber exercises. We opened the survey at ENISA's website from April 2012 until July 2012, and invited stakeholders in the global cyber exercise community to respond. The survey was filled in on a voluntary basis; therefore we cannot claim that we have covered all cyber-exercises.

---

[5] *An evaluation report from the exercise and a video are available online: http://www.enisa.europa.eu/act/res/ce2010*

[6] *http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/index_en.htm*

[7] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises*

[8] *The Cyber Europe 2012 Key findings report will be available (after Nov 2012) at:*

https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe

The final step in the process was the organisation of the *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises* on 27 June 2012 in Paris. In total, 17 speakers and approximately 65 participants, all involved in the field of cyber exercises, attended and contributed to the conference.

The objectives of the conference were to:

a) Exchange good practices in the field of international cyber crisis cooperation, specifically focusing on cyber exercises.
b) Bring together the stakeholders that organise and have experience in cyber exercises in order to explore cooperation between them.
c) Identify gaps and challenges in the field of international cyber crisis cooperation and in particular cyber exercises.

This report takes into account the results and recommendations of the 2012 Paris conference. The full details about the Conference, including the individual presentations, are available at ENISA's resilience and CIIP web pages.[9]

The data gathered from all three steps were analysed in order to draw valid conclusions about the nature of national and international cyber exercises. This report includes the results of this analysis.

In addition, ENISA has created a database[10] with the results of the open survey on the stocktaking of cyber exercises. Subsequently, we analysed the results of the stocktaking of cyber exercises. In this report we present the analysis of the results, the conclusions and recommendations.

Note that the data gathered in the three steps of our methodology were given to us on a voluntary basis. Therefore we cannot guarantee that these data correspond to a full mapping of all cyber exercises; i.e., we cannot claim we have an exhaustive list of all cyber exercises. We do believe, though, that we have the critical mass, covering a broad scope in terms of cyber exercise types.

1.4 Structure of the report

The rest of this report is structured as follows. Chapter 2 presents a general overview of the exercises in our research as well as the results from the open survey. It also contains a part focusing specifically on national cyber exercises in Europe. Chapter 3 presents the main findings, while the following chapter describes the main conclusions and sets out recommendations for future cyber exercises. The Annexes of the report contain the necessary supporting information and evidence.

[9] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-exercise-stocktaking/cyber-exercise-conference*

[10] *Restricted access though the ENISA Resilience portal*

2 Overview of cyber exercises

In this stocktaking we have collected information on a number of cyber exercises of national and international cyber exercises. The exercises studied display a mixture of different exercise types. In this section we present a general overview of our findings. Annex 1 and 2 provide more details on the results of the stocktaking.

2.1 Basic facts[11]

The number of exercises examined during this stocktaking was *85* (see the list of exercises in Annex 2), covering the period between 2002 and 2012. The data for these exercises were mainly taken from the open survey that ENISA had conducted over two months, as well as the related research we carried out. In our analysis we have included all the cyber exercises we found; in other words, there were no inclusion or exclusion criteria, as long as the event could qualify as a cyber exercise.

The number of European countries that participated in and organised national cyber exercises is 22. In total, 84 countries worldwide participated in the multinational exercises that we analysed.

2.2 General exercise information

Figure 1 shows the number of cyber exercises per year. We see that the majority of the exercises, around 71%, in this stocktaking were conducted in the last three years (2010–2012). ***This figure shows that governments and private organisations take cyber threats seriously.*** Based on the trend observed, we can expect the number of cyber exercises to increase in the coming years.

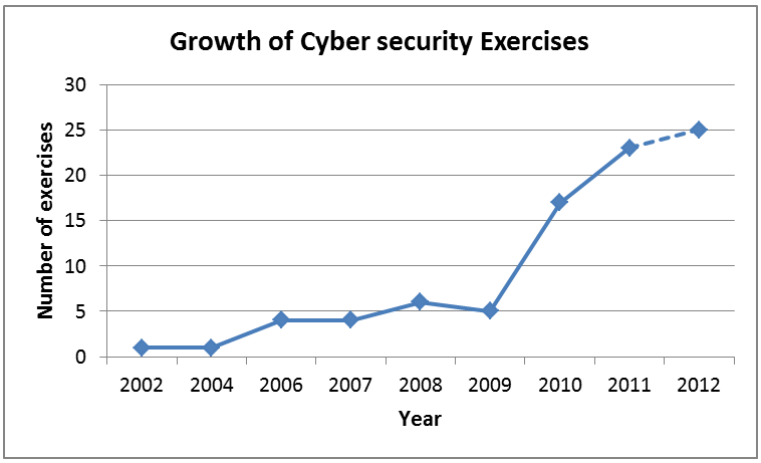


Figure 1: The cyber exercises collected by year

Figure 2 displays the duration of the cyber exercises we examined. We found that that 43% of the exercises were one-day events, 32% of the exercises continued for two to three days and 19% of the exercises took more than three days. We can see that approximately 75% (based on 81% of overall

[11] *Please note that the findings presented in this report are based on the exercises gathered in this stocktaking. Although the survey was open to all for a long period, scientifically we cannot claim this is an exhaustive research. It does, though represent a large sample.*

data gathered) of the exercises lasted for one to three days, which indicates that even a short period of time can be sufficient to execute a cyber exercise.

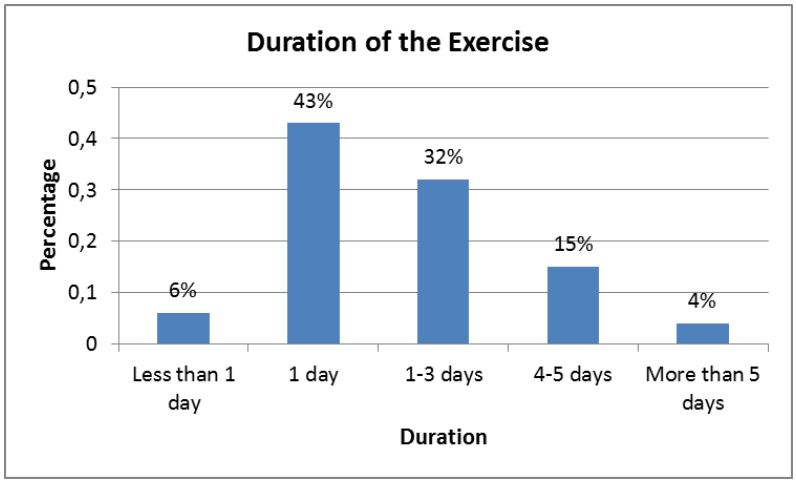


Figure 2: Duration of the cyber exercises examined

As Figure 3 shows, ***around 84% of the exercises (based on 82% of overall data gathered) are part of a series; around two-thirds of them take place on a yearly basis and a quarter on a biannual basis***.

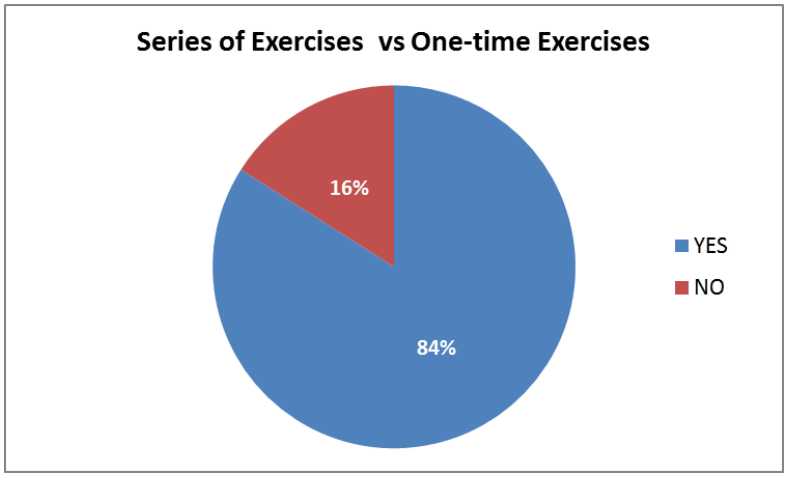


Figure 3: Proportion of exercises carried out as part of a series

2.3 Cyber exercises in Europe

More specifically, we looked at the situation of cyber exercises in Europe. Figure 4 shows the map of Europe and the number of national exercises organised by European countries. For this stocktaking, we included both EU and EFTA countries (31 countries in total).

According to our findings, between 2002 and 2012 six countries (indicated with ③ on the map) organised a national exercise three times. In the same period four countries (indicated with ② on the map) organised two national cyber exercises. The countries indicated with ① on the map conducted one national exercise. We thus see that 22 European countries have already organised one or more

national cyber exercise. Cyprus, Malta, Luxembourg and the Czech Republic have not yet conducted such an exercise. However, these countries were involved in international exercises.

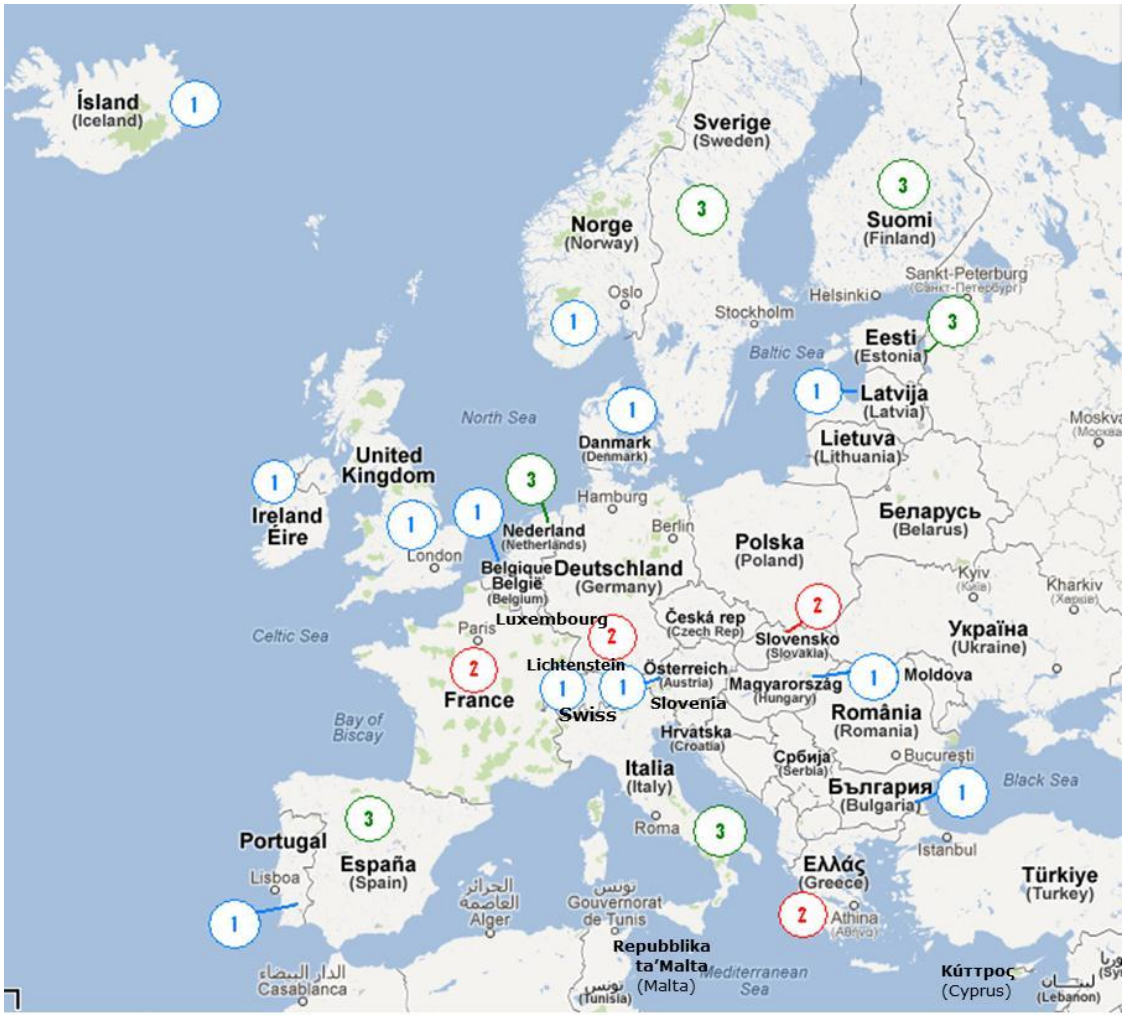


Figure 4: Cyber exercises in Europe for the period 2002–2012 (numbers indicate exercises per country)

Compared to data ENISA gathered in 2010, we observe a slight increase in the number of national and international cyber exercises in Europe (see Figure 5). Two years ago, 20 countries organised a national exercise.

This current stocktaking reveals that some countries have organised two or even three cyber exercises, while others have just completed one. In addition, almost all EU and EFTA countries have participated in multinational cyber exercises.

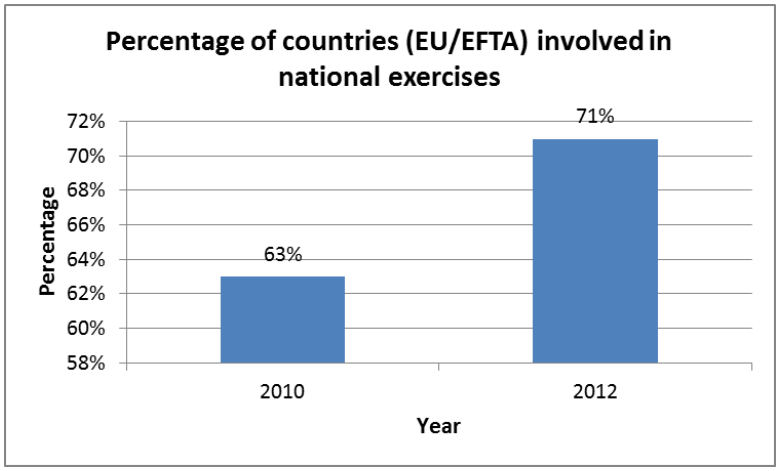


Figure 5: EU and EFTA countries involved in national cyber exercises; data from ENISA surveys of 2010 and 2012

2.4 Participation in cyber exercises

Figure 6 shows that approximately two-thirds of the exercises (based on 97% of overall data gathered) were national exercises and approximately one-third were multinational exercises. This indicates a tendency towards cooperation at the international level, even though matters of national security are usually domestic concerns. The cross border nature of cyber threats gives rise to the need for international cooperation. Based on these results, we anticipate that the trend of a growing number of multinational exercises will continue.

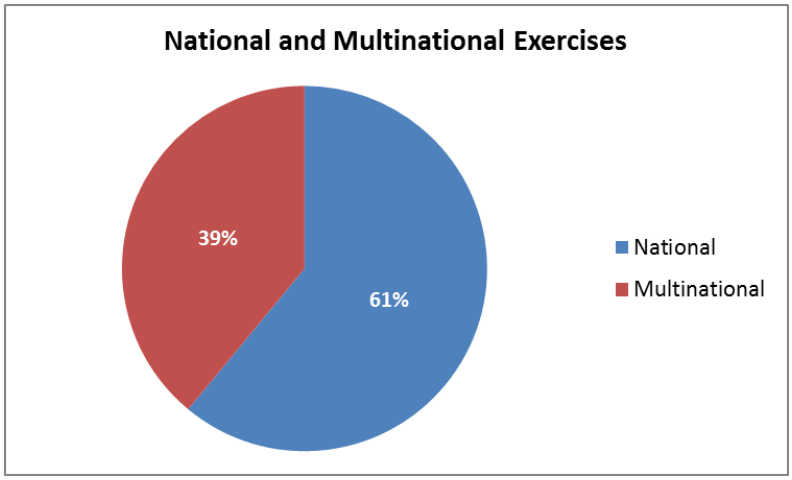


Figure 6: National vs. multinational exercises

In total, 64% (based on 94% of overall data gathered) of the multinational exercises involved more than 10 countries, 13% involved 6–10 countries and 13% involved 3–5 countries.

Another interesting aspect of cyber exercises is the participation of sectors, and more specifically the participation of the public and private sectors. As Figure 7 shows, we found that 57% of the exercises (based on 88% of overall data gathered) combined the public and private sector, while 41% involved only the public sector. We found that only one exercise in this stocktaking took place with only the private sector involved. This is an interesting finding that demonstrates that the private sector could be more proactive with testing security and contingency plans, as they are the owners of the

infrastructure and the actual experts in the subject. Public–private cooperation occurs in more than half of the exercises, which is attributed to the fact that private stakeholders play a critical role in the area of cyber crisis cooperation. As such, public–private cooperation in cyber exercises is likely to increase in the coming years.

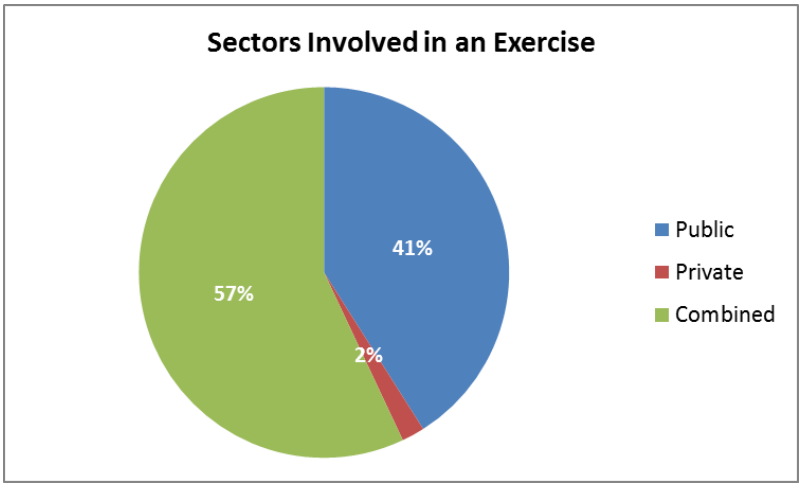


Figure 7: Sectors involved in the exercise

The number of participants in the exercises ranged from 20 to more than 75 people; this of course depends on the sectors and number of countries involved in the exercise.

2.5 Type of exercise

Many kinds of exercises exist, each with different formats, benefits, challenges and costs. There is no international standard taxonomy of exercise types, although there are many commonly used terms and categories (see table below). The simplest forms of exercise are the 'desk check' and 'walk through' exercises which use a simple scenario to validate a plan or procedures to ensure that the participants are able to meet the requirements of the organisation. The most complex are 'full simulation exercises' where players experience the pressure of working in real time responding to an unfolding scenario.

What	Why	How
Desk check	Early stage validation of a new plan or amendments to a plan.	One to one discussion with the author of the planned procedures against a simple scenario to demonstrate the stages that are in place and how they operate.
Comms check	To validate systems or infrastructures.	A different form of initial activity used to validate the communications methodologies or notification systems.
Walk through	The first time the response team convenes to consider the planned procedures and their roles.	The response team is convened in one room and a simple scenario is used to demonstrate the progression of the planned responses and what each responder should do.

Workshop	A scenario-based rehearsal of responses and actions in open forum, to allow discussion of activities.	A developmental step in the building of capability, using a scenario to rehearse in an open forum the responses of teams and actions without any time pressure.
Table-top	To validate plans and integration of procedures prior to moving on to more complex, team-based activities.	Scenario-based, open forum discussions with no external pressures. Responses are stepped through in a measured fashion and each aspect is discussed if needed before moving on.
Distributed table-top	To test plans and procedures.	Scenario-based, players act according to routine.
Command post	To enable a team to rehearse using their own response facilities. Usually only management level involvement.	Response centre based but with role play of the external environment and players.
Full simulation	To stress test the responses with a real time environment, as close to reality in every aspect as possible.	Players respond in real time as information is received, interacting with other teams and role players as the response requires.

As shown in Figure 8, 43% of the exercises (based on 61% of overall data gathered; the relevant data were not available for the remaining 39%) were executed as distributed table-top exercises (i.e. players remain in their usual place of work within their organisation/country); 19% were full simulation exercises; and 5% took the form of a workshop.

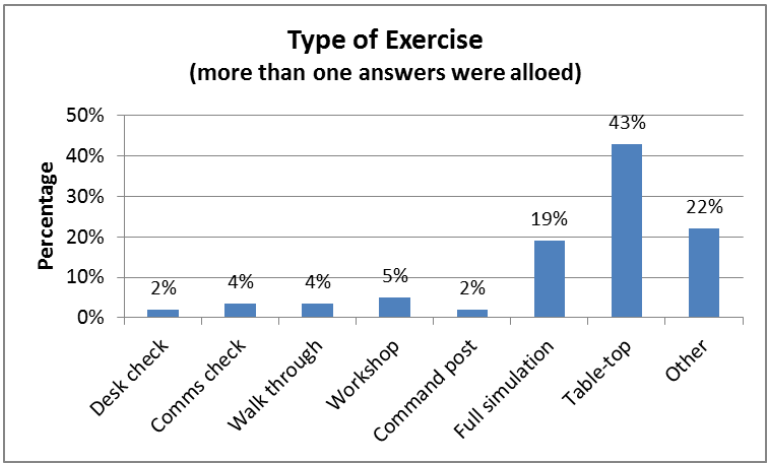


Figure 8: Types of cyber exercise

Figure 9 demonstrates that in total 48% of the exercises (based on 45% of overall data gathered) had an operational focus, while 17% were mainly tactical and 24% mainly strategic.[12] Most of the cyber exercises examined had a combined focus.

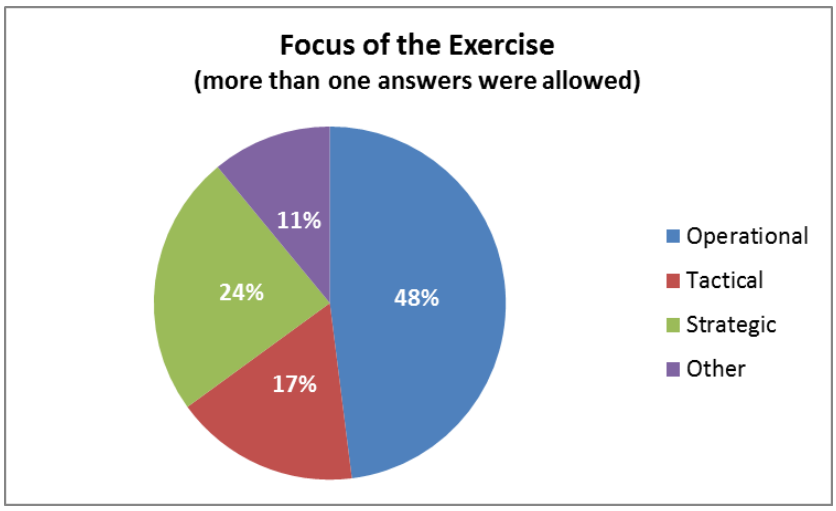


Figure 9: Focus of the exercise

Using the collected data, we see that most of the time a (distributed) table-top exercise was carried out. A (distributed) table-top is suitable for both beginners and experienced participants, and addresses the operational, tactical and strategic level.

2.6 Exercise execution

The following list shows which objectives were mentioned most often in the stocktaking survey:

- Build awareness about cyber threats;
- Examine the capabilities of participating organisations to prepare for, and respond to the effects of cyber-attacks;
- Identify and highlight roles, responsibilities and authorities for responding, as well as to test decision-making and procedures between public and private actors;
- Assess cyber security emergency readiness (prepare, test and evaluate (national) procedures and processes);
- Raise awareness of infrastructure interdependency issues with a particular focus on cyber security;
- Build trust among states; enhancing interstate and interagency cooperation.

As this list shows, raising awareness and building trust are important objectives of cyber exercises. In addition to the objectives, we found that procedures, plans, protocols, capabilities and players are all tested during the exercises.

Around half of the exercises (based on 25% of overall data gathered) made use of exercise management tools (i.e. tools and software to support preparation, execution and evaluation of an

[12] Operational *exercises focus mainly on checking technical issues;* tactical *exercises are mostly procedural tests; while* strategic *exercises refer mainly to high-level decision-making and policy exercises. A good reference for these terms is the ENISA* Good Practice Guide on National Cyber Contingency Plans (NCPs). *Please contact* resilience@enisa.europa.eu

exercise). However, ***three-quarters of all exercises gathered did not provide data about the exercise management tools.*** This could be either because they do not use tools, or because the information about them could be made public.

2.7 Monitoring and evaluation

Research shows there is a need for structured evaluation in order to improve the learning of participants in exercises. Looking only at outcomes of an exercise tends to undermine the aims of the exercise, is generally unfair to participants and encourages risk-avoiding behaviour. The focus should be on process characteristics that enhance the effectiveness of crisis management. Monitoring and evaluation tools help to structure feedback and formulate lessons learned.

The results of our stocktaking (illustrated in Figure 10) show that 31% of the exercises (based on 24% of overall data gathered) conducted real-time monitoring, 22% worked with status reports, and 27% employed experts to monitor the exercise. Most of these approaches are not used exclusively, and there are many exercises that use a combination of the different methods.

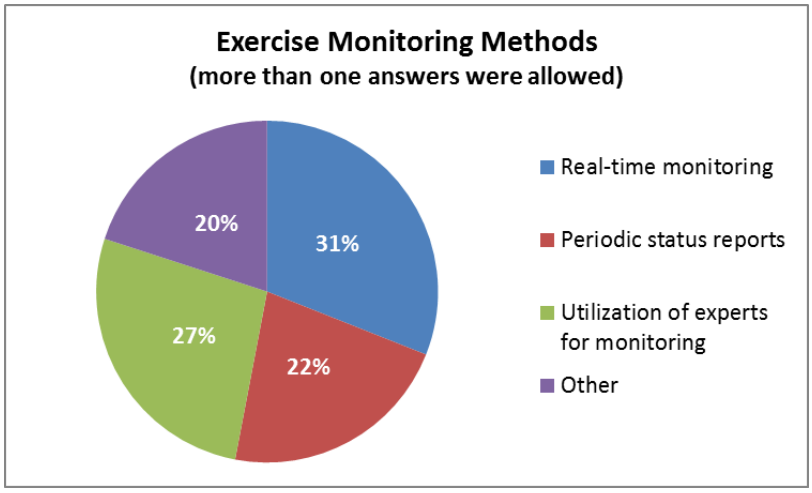


Figure 10: Type of monitoring methods used during or after the exercise

As demonstrated in Figure 11, we found that 16% of the exercises (based on 54% of overall data gathered) had a debriefing workshop, 31% made a report after the exercise, 17% had a hot wash session and 12% asked participants to carry out self-evaluation (with evaluation forms). Again in this case a combination of these evaluation methods is quite common policy.

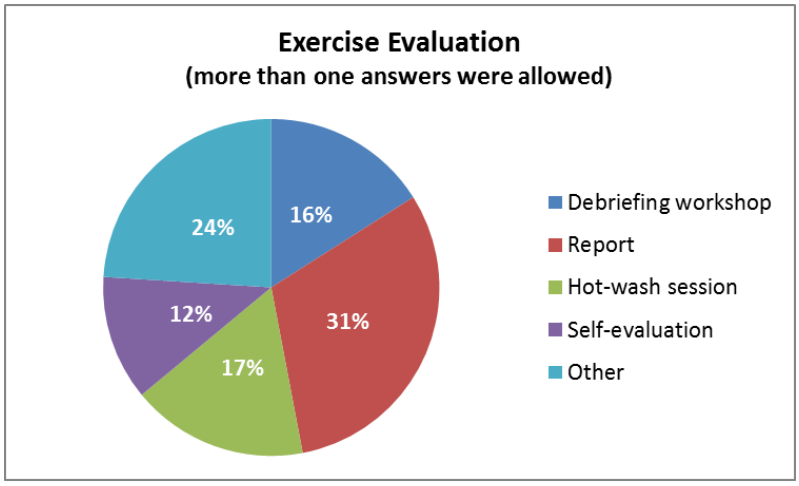


Figure 11: Cyber exercises evaluation

Using the collected data, we can see that a report of the exercise is made for most of the cyber exercises we have examined. This may be because exercise organisers need to report to their management about the exercise and the results.

2.8 Cyber exercises in the media

In 74% of the exercises (based on 67% of overall data gathered), the media reported about the exercises. Most media reports about these exercises are still available online.

The following list shows which type of information was mentioned most often in the media reports:

- The exercise was an excellent opportunity to enhance our nation's cyber security;
- The exercise organisers wanted to show they are working on their preparedness regarding cyber incidents;
- The outcomes of the exercise showed the need for further improvement of plans, and procedures;
- Several countries and organisations cooperated within the exercises;
- The exercise was a first examination of IT security;
- This exercise was a first step in organising regular exercises on critical information infrastructure protection as preparation against similar attacks.

As the list above shows, organising exercises attracts publicity for organisations and helps to raise awareness within a country about cyber security. In addition, media reporting about the exercise proved to have a positive impact on the reputation of organisations involved (e.g. that citizens learn about the work done by their government).

3 Summary of the main findings

This survey of national and international cyber exercises shows that countries engage in a variety of cyber exercises. The research presented in this report is not exhaustive as the results capture only 85 exercises of 84 countries (national or multinational, European or global) from 2002 to 2012.

However, we do think our stocktaking presents a good overview of the status quo and in this section we draw the main conclusions from the findings during our research. Below we have listed (in no particular order) the main findings.

1. The number of cyber exercises has increased in the past few years

Cyber exercises are becoming increasingly more common, with the number of exercises rising sharply since 2010. This may have been caused by the overall policy context that supports and boosts cyber exercises, cyber exercise and by the increasing threat of cyber incidents and attacks. Many exercises are part of an exercise series and take place on a yearly basis. This shows that interest and activity in the field of cyber exercises persists and that this trend will most likely continue in the coming years. We observed that many countries actively engage in this field and are preparing to carry out cyber exercises in the (near) future, both domestically and in international cooperation. In addition, the media seem to report more frequently on the cyber exercises.

2. Cyber crisis cooperation efforts are in constant development

Not only are cyber exercises more frequent and widespread, but there is also a constant development of cyber crisis cooperation initiatives. Cyber security is an urgent matter which receives increasingly more attention in European countries. The growing attention is spurred by the fact that societies face ever more complex and potentially devastating cyber-related contingencies and challenges. The participants in the *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises* stressed the need for more exchange of good practices in the area of cyber crisis cooperation (e.g. regarding exercises and conferences) in order to learn from each other's experiences, lessons and solutions.

3. Most European countries participate in national and multinational cyber exercises

Most EU and EFTA countries participate in both national and multinational exercises. This implies that efforts on a national level can be combined and complemented with efforts on a multinational level and that (inter)national cyber crisis cooperation expands during these exercises. For countries with limited national capacity (for instance to organise a national exercise), it is very helpful to participate in multinational exercises in order to ensure that their national preparedness meets the required standards. The fact that cyber crises do not stop at the border of a country also provides a strong incentive for larger countries to help neighbours with more limited capacity, and emphasises the need to jointly organise multinational exercises. ENISA supports these efforts by arranging seminars on cyber exercises[13] and pan-European regional exercises.[14]

4. Public–private liaison is essential due to private sector ownership of most critical information infrastructures

[13] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises

[14] https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe

Since many private sector stakeholders are involved in the protecting, managing and employing of critical information infrastructure, we consider it promising that private and public sector actors cooperate in many cyber exercises (about half of the exercises involve both public and private sector participants). However, the trend that critical information infrastructure is increasingly more owned by private stakeholders, shows the need to intensify public–private cooperation in cyber exercises in the future.

5. **More attention must be paid to exercise management tools**

The cyber exercise field seems to show an under-appreciation of exercise management tools. Exercise management tools can assist in exercise execution and preparation (e.g. when inexperienced people prepare to organise an exercise). During the *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises* several exercise management tools were presented and good practices were exchanged. However, the work in this area is still progressing and many exercises do not yet employ any exercise management tools. We believe the use of these tools will grow significantly and become more relevant in the years to come.

6. **Advance the use of planning, monitoring and evaluation methods**

Planning, monitoring and evaluation are crucial for exercise pay off, e.g. improvement of plans and procedures, policy changes, and planning and enhancement of new exercises. Planning is essential to guarantee an effective and successful exercise. It is crucial that organisers have enough time to plan, execute and evaluate exercises. The global cyber exercise community should exchange good practices regarding the planning process in order to help organisers prepare better for an exercise. The monitoring and evaluation process is made more efficient when good practices are shared among several exercise organisers. As this stocktaking yielded limited evidence of the use of monitoring and evaluation methods, we stress the fact that it is essential to gain ground in this respect. Monitoring and evaluation methods can further help exercise organisers to structure feedback and generate lessons learned.

4 Recommendations

Building on the findings from research on cyber exercises we have produced a number of recommendations that could increase the number and quality of cyber exercises, and thus contribute to the enhanced resilience of the critical cyber infrastructures and services.

The recommendations below[15] are mainly targeted at cyber exercise organisers, political leadership and policymakers, the various public agencies, national and international, behind the organisation and support of cyber exercises, the private sector owners of the cyber infrastructures, and the research and development community that can support the tools and methodologies for cyber exercises.

1. **Establish a more integrated cyber exercise community**
   As we observe the continuous expansion of the cyber exercise area and the constant development of the field of cyber crisis cooperation, there is a need for a more integrated cyber exercise community in which good practices, challenges and lessons learned are exchanged and discussed among stakeholders in the global field of cyber exercises. Most of the current efforts, such as national cyber exercises and multinational, civilian and cyber defence, are quite segregated. A big challenge for the cyber community is to coordinate the exercise schedules, and synchronise wherever possible, in order to be able to learn from each other. In addition, we recommend continuing with the organisation of international conferences in the field of cyber crisis cooperation in order to build a more integrated cyber exercise community.

2. **Exchange of good practices on cyber exercises – public–private cooperation**
   The *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises* provided a number of ideas about how to share good practices in the field of cyber exercises. The most important recommendation is the need for cooperation between the private and public sector. *Private–public partnerships*[16] for the protection of critical information infrastructures are very important, and in that context joint exercises and sharing of best practices are essential. Other suggestions for exchanging good practices include: the establishment of (virtual) databases for sharing good practice in conducting cyber crisis exercises and observing each other's exercises in order to learn from them and exchange ideas. We recommend that all stakeholders in the global field of cyber exercises engage in the exchange of good practices and that private–public partnerships are established and utilised for cyber exercising. ENISA will aim to facilitate this in the future.

3. **Further development of the area of exercise management tools to support exercise organisation**
   The planning, execution and evaluation processes of cyber exercises can be more efficient if they use well defined methodologies and automated tools to support them. Exercise management tools, including simulators and emulators, can help advance these processes and improve exercise quality and outcome. We urge the global cyber exercise community to support the development, adoption and sharing of exercise management tools.

[15] *Given in no particular order.*

[16] *http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership*

4. **Aim for more complex cyber exercises on an inter-sectoral, international and European level**
   One of the main challenges we found during our research on cyber exercises is the cross-border nature of most of the cyber incidents/crises. These types of crises cross the boundaries of countries, and sectors. The challenge is to organise cyber exercises that can test all different complexities of a cross-border crisis, specifically testing different levels (operational, tactical and strategic) together. We recommend the global cyber exercise community, together with ENISA, aims for more complex exercises.

5. **Enhance preparedness by including exercises in the lifecycle of Cyber Crisis Contingency Plans**
   Countries need to develop, maintain and update their crisis contingency plans and standard operational procedures for cooperation. The continuous improvement of the response structure (as described in the crisis contingency plans) is refined and fuelled by performing exercises. We recommend that policymakers in the EU Member States include exercises in cyber crisis contingency plans and standard cooperation procedures, since this enhances their preparedness for cyber crises. ENISA prepared a *Good Practice Guide on National Cyber Contingency Plans*.[17] We recommend the use of this guide in the development of a coordinated response and crisis management of large-scale cyber incidents.

6. **Update the good practices for national exercises and promote good practices for multinational exercises**
   In 2009, ENISA developed a *Good Practice Guide on National Exercises*[18] as is a first step towards a more formal methodology for planning and conducting cyber exercises. Another related effort is the HERMESOEx method.[19] We recommend these methods are merged and updated by ENISA based on developments in recent years in the European policy area, the results gathered in this research and the forums such as the *1st International Conference on Cyber Crisis Cooperation: Cyber Exercises,* and create a formal method, with the relevant tools, for planning and organising cyber exercises.

7. **Develop feedback mechanisms for ensuring that lessons learned from cyber exercises are implemented resulting in enhanced cyber crisis preparation**
   Any cyber exercise (an exercise in general) is not a target in itself. A cyber exercise is considered part of the preparedness and response procedures development and maintenance lifecycle. Therefore it is vital to have the necessary feedback mechanisms to implement any changes needed as a result of the lessons learned from the exercise. These mechanisms include both the appropriate feedback tools analytical evaluation reports on preparedness, cooperation and response improvement, but also political and strategic empowerment of the owners of processes and procedures to allow them to proceed with the implementation of changes with the appropriate resources. Both aspects are considered essential for the success of an exercise.

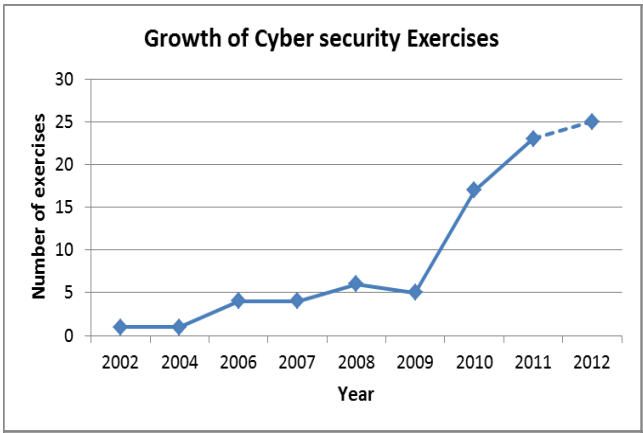
---

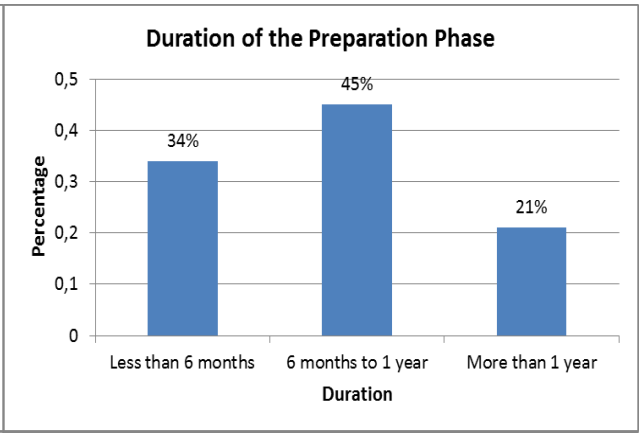
[17] *The ENISA* Good Practice Guide on National Cyber Contingency Plans *is available upon request.*

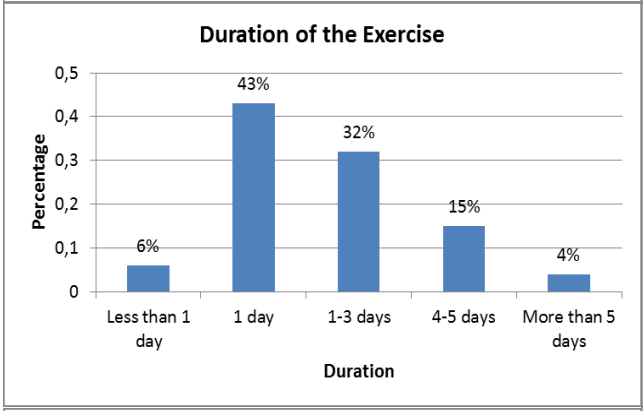
[18] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises

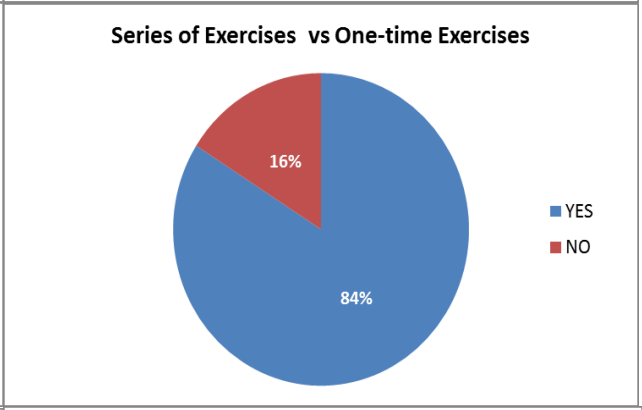
[19] http://www.hermes.admin.ch/services-en/hilfsmittel/hermes-for-the-organisation-of-exercise-projects-hermes-oex?set_language=en&cl=en

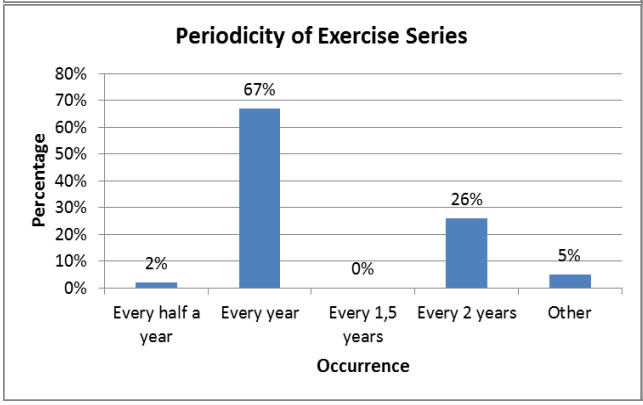
ANNEX 1: Full results of the survey

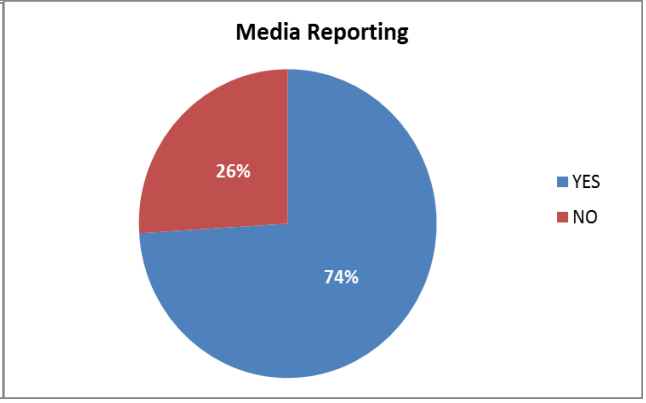




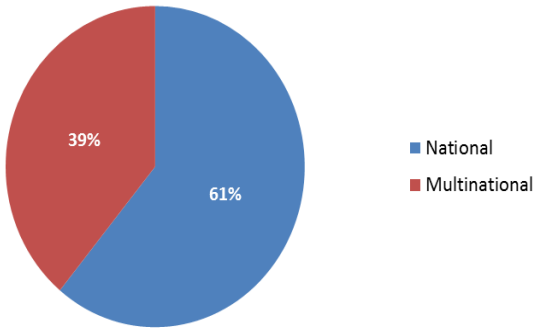




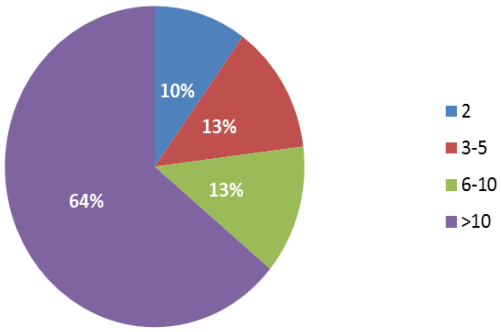




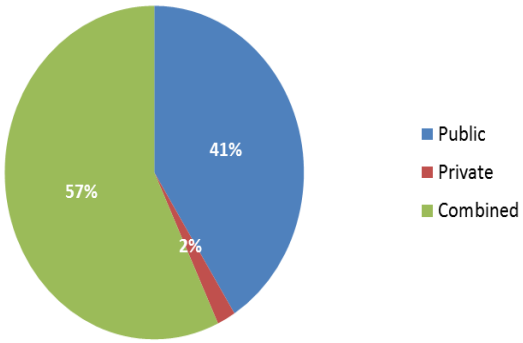
National and Multinational Exercises



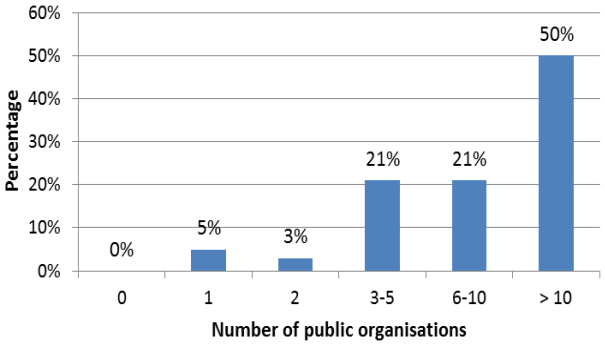
Number of Countries in Multinational Exercises



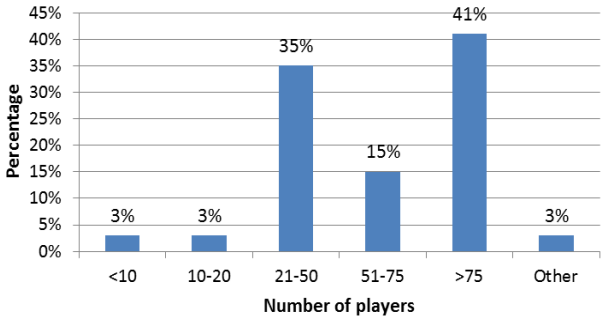
Sectors Involved in an Exercise



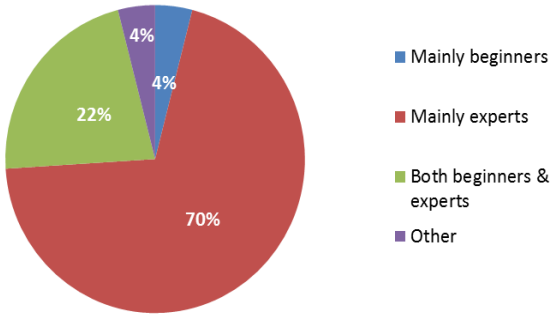
Number of Public Organisations in the Exercise



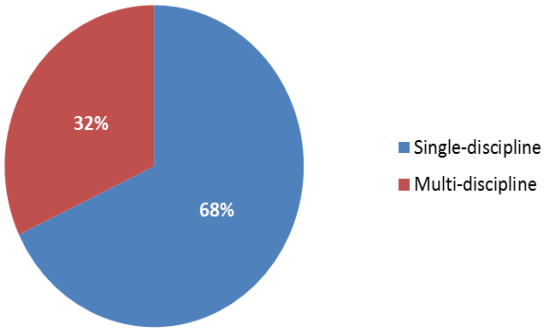
Number of Players in an Exercise



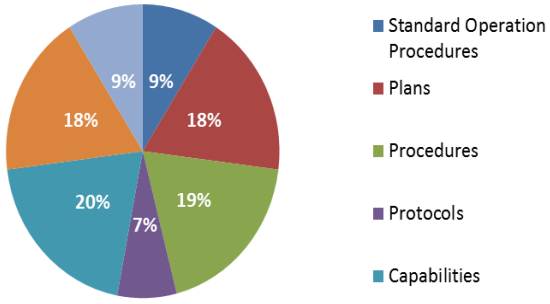
Level of Players' Experience

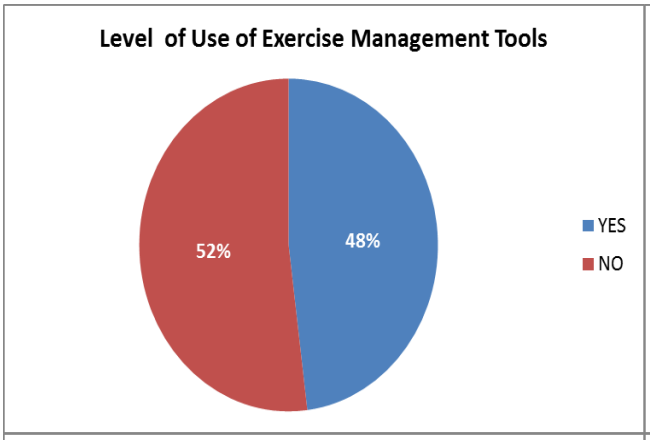


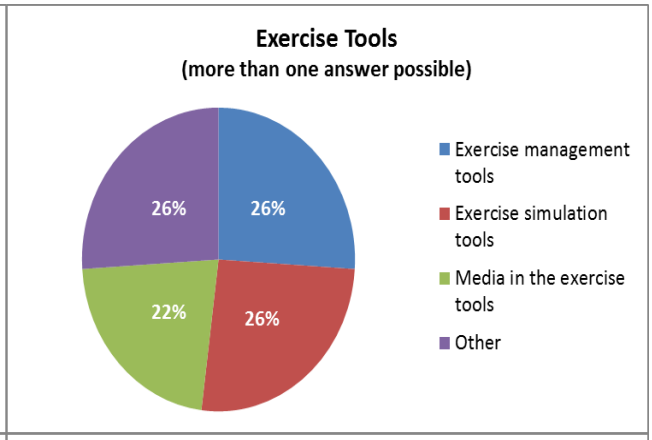
Single-discipline vs Multi-discipline Exercises

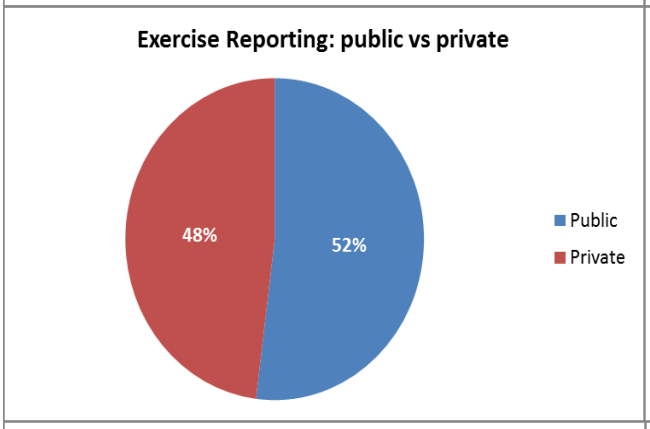


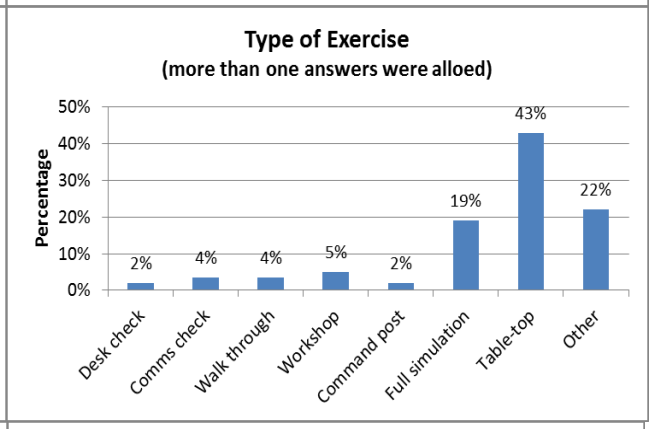
Measures Tested During the Exercise
(more than one answer possible)

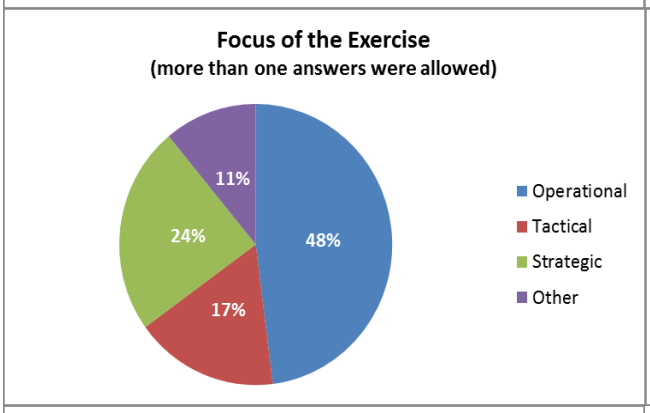


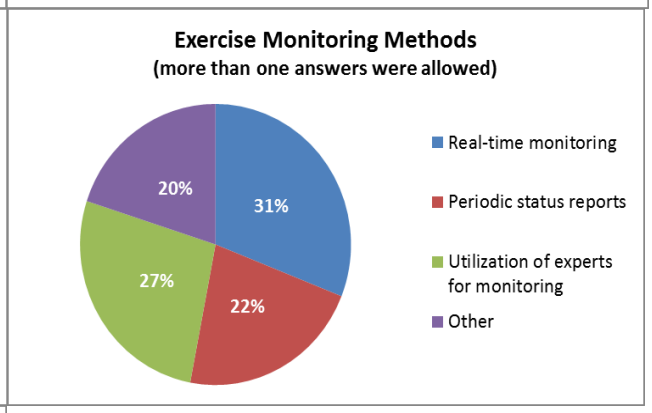

Level of Use of Exercise Management Tools
48%
52%
YES
NO

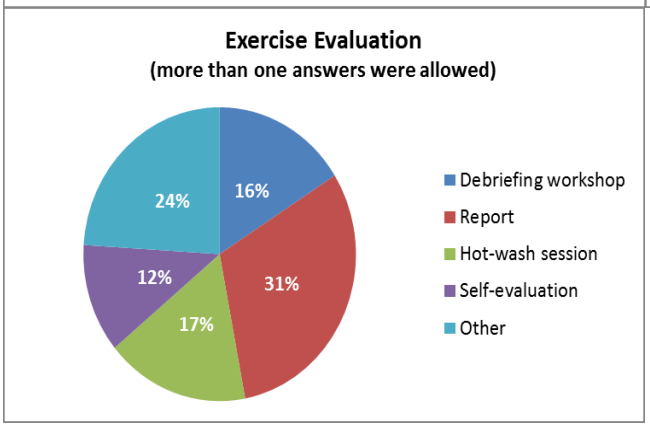

Exercise Tools
(more than one answer possible)
26%
26%
22%
26%
Exercise management tools
Exercise simulation tools
Media in the exercise tools
Other


Exercise Reporting: public vs private
48%
52%
Public
Private


Type of Exercise
(more than one answers were alloed)
Percentage
50%
40%
30%
20%
10%
0%
2%
4%
4%
5%
2%
19%
43%
22%
Desk check
Comms check
Walk through
Workshop
Command post
Full simulation
Table-top
Other


Focus of the Exercise
(more than one answers were allowed)
11%
24%
48%
17%
Operational
Tactical
Strategic
Other


Exercise Monitoring Methods
(more than one answers were allowed)
20%
31%
27%
22%
Real-time monitoring
Periodic status reports
Utilization of experts for monitoring
Other


Exercise Evaluation
(more than one answers were allowed)
24%
16%
12%
31%
17%
Debriefing workshop
Report
Hot-wash session
Self-evaluation
Other

ANNEX 2: List of the cyber exercises from the survey

	YEAR	EXERCISE	LOCATION
1	2002	Blue Cascades I	**Welches, OR, USA**
2	2004	Blue Cascades II	**Seattle, WA, USA**
3	2006	ASEAN CERT Incident Drills (ACID 2006)	
4	2006	Cyberstorm I	**USA**
5	2006	FY 2006	**Japan**
6	2006	NICTer Project 2006	**Japan**
7	2007	ASEAN CERT Incident Drills 2007 (ACID 2007)	
8	2007	APCERT Drill 2007	
9	2007	FY 2007	**Japan**
10	2007	Shift Control	**The Netherlands**
11	2008	APCERT Drill 2008	
12	2008	Cyber Coalition 2008	
13	2008	Cyberstorm II	**USA**
14	2008	FiCom 2008	**Finland**
15	2008	FY 2008	**Japan**
16	2008	IKT 08 (ICT 08)	**Norway**
17	2009	APCERT Drill 2009	
18	2009	Cyber Coalition 2009	
19	2009	FiCom 2009	**Finland**
20	2009	FY 2009	**Japan**
21	2009	White Noise	**UK**
22	2010	10th Annual Cyber Defense Exercise	**Greenbelt, ML, USA**
23	2010	APCERT Drill 2010	
24	2010	Baltic Cyber Shield 2010	
25	2010	COM 10-1	**Germany**
26	2010	Cyber Coalition 2010	**Mons, Belgium**
27	2010	Cyber Europe 2010	
28	2010	Cyber Hedgehog 2010	**Estonia**

29	2010	Cyberstorm III	**USA**
30	2012	Cyberstorm III-NL pact	**The Hague, Netherlands**
31	2010	ECD – Ejercicio de Cyberdefensa 2010	**Spain**
32	2010	FY 2010	**Japan**
33	2010	Gaillean Exercise	**Ireland**
34	2010	Nationell informationssäkerhetsövning (NISÖ)	**Sweden**
35	2010	Panoptis 2010	**Greece**
36	2010	PHOENIX 2010	**Sofia, Bulgaria**
37	2010	Piranet 2010	**France**
38	2010	Tallinn CIIP 2010	**Tallinn, Estonia**
39	2011	APCERT Drill 2011	
40	2011	CERT.LV Technical IT Security Exercise 2011	**Latvia**
41	2011	COMEX	**Hungary**
42	2011	Copy…Paste	**The Hague, Netherlands**
43	2011	Cyber Atlantic 2011	**Lisbon, Portugal**
44	2011	Cyber Coalition 2011	
45	2011	CYBER DEFENCE 2011	**Germany**
46	2011	Cyber Endeavor	**Grafenwöhr, Germany**
47	2011	Cyber Italy 2011	**Italy**
48	2011	CYBER WINTER 2011	**Bulgaria**
49	2011	ECD – Ejercicio de Cyberdefensa 2011	**Spain**
50	2011	EuroCybex 2011	
51	2011	FY 2011	**Japan**
52	2011	HACKCERT 2011	**Italy**
53	2011	Information Security Exercise 2011	**Slovakia**
54	2011	ITU IMPACT ALERT 2011	
55	2011	KRISESTYRINGSØVELSE 2011	**Denmark**
56	2011	LÜKEX 2011	**Germany**
57	2011	(Malaysia) National Cyber Security Exercise	**Malaysia**
58	2011	Panoptis 2011	**Greece**

59	2011	Slovak Information Security Exercise (SISE)	**Slovakia**
60	2011	Telö 11	**Sweden**
61	2011	Turkish National Cyber Security Exercise 2011	**Turkey**
62	2011	Operation Kill Switch	**USA**
63	2012	APCERT Drill 2012	
64	2012	BelgoCybex	**Belgium**
65	2012	COMPOR 2012	**Portugal**
66	2012	Cyber Defense Exercise 2012 (CDX 2012)	**USA**
67	2012	Cyber Europe 2012	
68	2012	Cyber Fever 2012	**Estonia**
69	2012	Cyber Italy 2012	**Italy**
70	2012	Cyber Phalanx	
71	2012	Cyber Planspiel	**Austria**
72	2012	Cyberstorm IV	**USA**
73	2012	EuroSOPEx	
74	2012	Eventide	**Los Alamos, NM, USA**
75	2012	ITU-IMPACT 2012	**Amman, Jordan**
76	2012	Jornadas PSCIC	**Spain**
77	2012	Lights Out 2012	**Israel**
78	2012	Locked Shields 2012	
79	2012	National Crisis Management Exercises	
80	2012	Netútlaginn 2012	**Iceland**
81	2012	NLE 2012	**USA**
82	2012	Piranet 2012	**France**
83	2012	Switzerland Cyber Exercise	**Switzerland**
84	Every half year	TIETO	**Finland**
85	No date provided	PTS Trainings	**Sweden**

P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu