Cyber exercises taxonomy
This study has been written with the coordination and participation of Elena García Díez, Daniel Fírvida Pereira, Marco A. Lozano Merino, Héctor R. Suárez and Darío Beneitez Juan.

March 2015
INDEX

1  INTRODUCTION........................................................................................................... 5

1.1  ACRONYMS.................................................................................................................. 6

2  WORKING METHODOLOGY ....................................................................................... 6

3  IDENTIFICATION AND ANALYSIS OF CYBEREXERCISES ................................. 9

3.1  INFORMATION GATHERING......................................................................................... 10

3.2  AVAILABLE INFORMATION ...................................................................................... 11

3.3  METRICS ..................................................................................................................... 13

3.4  CYBER EXERCISES PROFILING ............................................................................... 14

   3.4.1  Participation of countries in cyber exercises ......................................................... 14

   3.4.2  Sectors Involved .................................................................................................... 20

   3.4.3  Cyber exercises modality ..................................................................................... 23

   3.4.4  Time Pattern of cyber exercises .......................................................................... 24

   3.4.5  Cyber exercises included in the Digital Agenda for Europe ................................ 26

   3.4.6  Indecent phases covered by cyber exercises ......................................................... 27

   3.4.7  Participation level of EU countries in international cyber exercises .................. 28

4  CYBER EXERCISES: PROPOSED TAXONOMY ................................................. 29

4.1  FOCUS ......................................................................................................................... 31

4.2  MODEL ......................................................................................................................... 32

4.3  VERTICAL SECTOR .................................................................................................... 34

4.4  SCOPE FOR PARTICIPATION .................................................................................... 35

4.5  DISSEMINATION OF RESULTS ................................................................................ 36

5  TAXONOMY APPLICATION IN CYBER EXERCISES ...................................... 37

5.1  SELECTION OF CYBER EXERCISES ....................................................................... 37
5.2 APPLICATION OF TAXONOMY

5.2.1 Sectorial Perspective

5.2.2 Used Models

5.2.3 Situation in Spain

6 CONCLUSIONS

7 LISTS AND REFERENCES

7.1 LIST OF FIGURES

7.2 LIST OF TABLES
1 INTRODUCTION

Although John Dewey is considered the intellectual origin of simulation engineering, through his "Education and Experience" (1938, New York, Collier), where he argued against excess theory. The idea of designing simulated environments for teaching was still a novelty in the late '60s. This issue was considered as a learning process, and was established between an educator to students on a particular topic, using the accepted means (books, conferences, etc.).

However, in the 60s the REFORGE Exercise (back to Germany) is already mentioned, which was first conceived in 1967 by the North Atlantic Treaty Organisation (NATO), and hold annually during the Cold War. Its aim was to test the ability to deploy forces to West Germany in the event of a conflict with the Warsaw Pact quickly.

From the 80, the simulation is becoming increasingly important as a means of training, and it can be said that it is a tool that provides the ability to perform, in a safe and controlled manner, a similar practice to that which would be performed in reality to some situations during their execution.

Moved to the cyber point of view, we can define a cyber exercise as a tool to assess the readiness of participants versus cybernetic origin crisis, also facilitating learned lessons and recommendations for the future: areas for improvement against a cyber attack, for increasing cooperation and coordination within sectors involved, for interdependencies identification, for awareness and training improvement, etc.

Although the number of cyber exercises performed annually between 2002 and 2004 were reduced, its celebration has considerably grown in recent years, regarding purpose, geographical scope, number of sectors involved and participation profile.

As an example, Chapter 3 of this document presents those cyber exercises, that have been collected and identified, taking into account the methodology used for this project.

Their classification would allow a greater understanding of its current status, and would become a tool for understanding and planning the embodiments thereof, both public and private.

Therefore, this paper proposes a taxonomic classification scheme for cyber exercises, based on the information collected, which is described in Chapter 4. The taxonomy is applied to cyber exercises that were considered the most relevant, in Chapter 5 of this document.

1 http://www.labsag.co.uk/es/index.php/simuladores-de-negocios/historia-y-eficacia-de-la-simulacion/
1.1 ACRONYMS

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APCERT</td>
<td>Asia Pacific Computer Emergency Response Team</td>
</tr>
<tr>
<td>APEC</td>
<td>Asia-Pacific Economic Cooperation</td>
</tr>
<tr>
<td>CERT</td>
<td>Computer Emergency Response Team</td>
</tr>
<tr>
<td>EGC</td>
<td>European Government CERTs</td>
</tr>
<tr>
<td>ENISA</td>
<td>European Network and Information Security Agency</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communications Technology</td>
</tr>
<tr>
<td>NATO</td>
<td>North Atlantic Treaty Organization</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
</tbody>
</table>

Table 1. Acronyms

2 WORKING METHODOLOGY

The aim of this document is to present a proposal for a taxonomy of cyber exercises, and applying it to those cyber exercises considered more relevant. The taxonomy can become a useful tool for the national and international cybersecurity community, providing a better understanding of existing cyber exercises, as well as helping to plan future editions.

Taxonomy means the classification of items in groups with common characteristics. According to this definition, the application of a cyber exercises taxonomy will provide their characterization, and will facilitate the identification of current gaps on their execution, through the analysis of the application of the taxonomy, to those cyber exercises, which have been considered the most relevant.

To this aim, the first step has been *information gathering* and analysis of available information about the different cyber exercises that have been held to date. Along this document, the concept “cyber exercise” will be used to refer to any edition in time. For example, if different cyber exercises have been held under the name “*Cyber Storm*”, each edition has been considered as a different cyber exercise.

After the analysis of the information, it has been developed a taxonomy of cyber exercises for the identified cyber exercises. This has been subsequently applied to those cyber exercises considered to be relevant based on predetermined criteria. Next figure depicts the working methodology:
During the first phase, as much public information about existing cyber exercises as possible has been attempted to be gathered. For this purpose, there have been used
different sources, including the Digital Agenda for Europe, the *European Union Agency for Network and Information Security* (ENISA). As well as online desktop research, of the web references listed in this document, which was carried out on 5 September 2014.

Once information had been gathered, a set of metrics and indicators had been defined. The results of applying these metrics were analyzed in order to establish a cyber exercises profiling, which shows different characteristics found on their execution, and facilitates the later taxonomy definition. Additionally, the completeness of information gathered were reviewed, in order to take into account that the analysis results depend on the quantity of information that had been possible to be collected.

On the basis of the cyber exercises analysis and profiling, and taking as a point of reference the studies carried out by organizations from different geographic scope, related to cyber exercises classification, a taxonomy proposal has been developed, to be used by both the public and private sectors for a better planning and improvement of future cyber exercises.

Finally, the cyber exercises taxonomy has been applied to the relevant cyber exercises that were been identified after applying the metrics, in order to disclose the usefulness of the taxonomy, and to reach some conclusions which could lead to a deeper knowledge of the current state of cyber exercises, and enhance the planning of future ones.
3 IDENTIFICATION AND ANALYSIS OF CYBEREXERCISES

This chapter presents the information gathered about the different cyber exercises that have been identified from the information sources, including the Digital Agenda for Europe, ENISA, and online investigation.

Next figure depicts the working methodology aspects that will be addressed in this chapter.

Firstly, it is described the process for gathering public information, as well as the information sources that have been used for this purpose.
Although complete information on each of them is not always available, the first point is followed by the description of the completeness of information collected about every cyber exercise. The goal of this aspect is to highlight that the results of the cyber exercises study could be conditioned by the amount of public information that was possible collected. Moreover, this will become a selection criteria to choose the more relevant cyber exercises, so that cyber exercises with more information available will become more probable candidates for applying the taxonomy.

3.1 INFORMATION GATHERING
The first source of information that has been used is the Digital Agenda for Europe\(^2\). For its implementation in member states, the action 39\(^3\) that belongs to the pillar of "trust and confidence" and it is related to the participation of states in cyber exercises, and planning future participations.

Information on the above implementation is published on a web page with data is updated either by the representatives of the member states (subscribers), or by anyone who wants to provide relevant information via online. With this information, it has been possible to establish the initiatives addressed by European countries in relation to the cyber exercises they have made, both nationally and internationally.

Another important source of information has been ENISA\(^4\). This organization published a paper in 2012\(^5\), which contains a catalogue of cyber exercises hold between 2002 and 2012. To this aim, they conducted two types of activities: firstly, they collected information on cyber exercises for 6 months, both in papers, desktop research and online sources, and secondly, they conducted a survey on the different existing cyber exercises, in order to gather information through the contacts of the agency itself.

It is significant that ENISA cannot confirm that the information obtained is complete and current. Therefore, in this paper we have made a new personalized search for cyber exercises previously treated by ENISA, identifying and updating editions, in an attempt to complete the information previously reported in the ENISA report.

Furthermore, in order to facilitate the harmonization of cyber exercises classification, there have been taken into account classifications made by the working group of telecommunications and information of Asia-Pacific Economic Cooperation (APEC)\(^6\), besides having considered the fields previously used by ENISA in gathering information.

\(^2\) [http://ec.europa.eu/digital-agenda/]
\(^4\) [http://www.enisa.europa.eu/]
\(^6\) [http://www.apec.org/]
Finally, regarding information gathering, there were conducted a research on various online sources, which allowed to complete and update the catalogue of cyber exercises developed in the period 2012-2014, prioritizing both, new cyber exercises and those one that introduce differentiating elements compared to previously identified, such as its focus, or the participation of new sectors.

3.2 AVAILABLE INFORMATION
The information that is available and has been gathered about each cyber exercise, presents varying degrees of detail. For example, in the report by ENISA used as a reference, identification of every cyber exercise prevails over the degree of detail of each one of them.

Another important aspect to be considered is that the cyber exercises organizers do not always provide all of the information about them, treating this information occasionally as sensitive information, not publicly available.

Taking this into account, the completeness of the information for each cyber exercise was evaluated, in order to highlight that the obtained results are dependent upon the information that has been possible to collect about them.

To make this assessment, the following criteria for the completeness of the information was followed:

- **High**: when the quantity and quality of collected information is considered sufficiently complete, accurate and up to date with the latest cyber exercises.

- **Medium**: when information is collected to date, but is not considered to have sufficient quality or quantity to provide a complete view of the cyber exercise.

- **Low**: when collected information is considered to be outdated, or very little information is available.

The following table summarizes the assessment of the completeness of information that has been collected for each group of cyber exercises identified. A group of cyber exercises means those ones that have the same name (for instance Cyber Storm), regardless of the number of cyber exercises celebrated over time.

<table>
<thead>
<tr>
<th>EXERCISE</th>
<th>COMPLETENESS OF INFORMATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>BLUE CASCADES</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER STORM</td>
<td>High</td>
</tr>
<tr>
<td>GRIDEX</td>
<td>High</td>
</tr>
<tr>
<td>ASEAN CERT INCIDENT DRILL</td>
<td>Medium</td>
</tr>
<tr>
<td>APCERT DRILL</td>
<td>Medium</td>
</tr>
<tr>
<td>Exercise</td>
<td>Level</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>-------</td>
</tr>
<tr>
<td>ITU IMPACT</td>
<td>Medium</td>
</tr>
<tr>
<td>BALTIC CYBER SHIELD CYBER DEFENCE EXERCISE</td>
<td>High</td>
</tr>
<tr>
<td>LOCKED SHIELDS</td>
<td>High</td>
</tr>
<tr>
<td>PHOENIX</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER ENDEAVOR</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER CRISIS MANAGEMENT</td>
<td>Low</td>
</tr>
<tr>
<td>CYBER COALITION</td>
<td>Low</td>
</tr>
<tr>
<td>CYBERATLANTIC</td>
<td>Low</td>
</tr>
<tr>
<td>CYBEREUROPE</td>
<td>Medium</td>
</tr>
<tr>
<td>EUROCYBEX</td>
<td>High</td>
</tr>
<tr>
<td>EUROSOPEX</td>
<td>Low</td>
</tr>
<tr>
<td>CYBER-EX</td>
<td>Medium</td>
</tr>
<tr>
<td>PSCIC</td>
<td>Medium</td>
</tr>
<tr>
<td>EJERCICIO DE CIBERDEFENSA</td>
<td>Low</td>
</tr>
<tr>
<td>CYDER</td>
<td>Medium</td>
</tr>
<tr>
<td>FIRST CYBERSECURITY WAR GAMES</td>
<td>Low</td>
</tr>
<tr>
<td>SHIFT-CONTROL EXERCISE</td>
<td>Low</td>
</tr>
<tr>
<td>PANOPTIS</td>
<td>Medium</td>
</tr>
<tr>
<td>PIRANET</td>
<td>Low</td>
</tr>
<tr>
<td>NATIONAL CYBER SECURITY EXERCISE</td>
<td>High</td>
</tr>
<tr>
<td>LÜKEX</td>
<td>High</td>
</tr>
<tr>
<td>BELGOCYBEX</td>
<td>Low</td>
</tr>
<tr>
<td>CYBER ITALY</td>
<td>Low</td>
</tr>
<tr>
<td>EVENTIDE</td>
<td>Low</td>
</tr>
<tr>
<td>CYBER DEFENSE EXERCISE</td>
<td>High</td>
</tr>
<tr>
<td>OPERATION KILL SWITCH</td>
<td>Low</td>
</tr>
<tr>
<td>NATIONAL LEVEL EXERCISE</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER CHALLENGE</td>
<td>Medium</td>
</tr>
<tr>
<td>COLLEGIATE CYBER DEFENSE COMPETITION</td>
<td>Medium</td>
</tr>
<tr>
<td>QUANTUM DAWN</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER AND OPERATIONAL RESILIENCE</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER ATTACK PAYMENT PROCESSES</td>
<td>Medium</td>
</tr>
<tr>
<td>CYBER GUARD</td>
<td>Low</td>
</tr>
<tr>
<td>CYBERRX</td>
<td>High</td>
</tr>
<tr>
<td>ENRIC</td>
<td>Low</td>
</tr>
<tr>
<td>GESTIÓN DE CRISIS DE CIBERSEGURIDAD</td>
<td>Low</td>
</tr>
<tr>
<td>WAKING SHARK</td>
<td>Medium</td>
</tr>
<tr>
<td>WHITE NOISE</td>
<td>Medium</td>
</tr>
<tr>
<td>COMEX</td>
<td>Low</td>
</tr>
<tr>
<td>SLOVAK INFORMATION SECURITY EXERCISE</td>
<td>Medium</td>
</tr>
<tr>
<td>POST AND TELECOM AGENCY</td>
<td>Medium</td>
</tr>
</tbody>
</table>
3.3 METRICS
The main objective of defining metrics is to evaluate and monitor security status, with the aim of undertaking improvement actions.

In addition to metrics, we can define indicators, which are the result of applying an analytical model to one or more metrics, in connection with some objective criteria. If the target criteria is defined, such as 100%, the corresponding indicator will tell us how we are approaching this target value.

In this chapter, a number of metrics have been defined in order to present a cyber exercises profiling, as well as to outline conclusions.

Both individual metrics by cyber exercise, and global metrics have been considered. Each metric is associated with its corresponding indicator, which is the result of comparing that metric with a target value, becoming useful information for cyber exercises profiling.

The following tables list the metrics that have been considered and their associated indicator.

<table>
<thead>
<tr>
<th>METRICS BY CYBER EXERCISE</th>
<th>INDICATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. countries involved/cyber exercise</td>
<td>Participation of countries in cyber exercises</td>
</tr>
<tr>
<td>No. EU countries involved/cyber exercise</td>
<td>EU Participation in cyber exercises</td>
</tr>
<tr>
<td>No. entities or organizations involved/cyber exercise</td>
<td>Participation of entities in cyber exercises</td>
</tr>
<tr>
<td>No. vertical sectors involved/cyber exercise</td>
<td>Vertical sectors involvement in cyber exercises</td>
</tr>
</tbody>
</table>

Table 3. Metrics by cyber exercise and associated indicator
### Table 4. Global metrics and associated indicators

<table>
<thead>
<tr>
<th>GLOBAL METRICS</th>
<th>INDICATOR</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. International cyber exercises with EU participant countries</td>
<td>EU participation in international cyber exercises</td>
</tr>
<tr>
<td>No. cyber exercises with Spanish participation</td>
<td>Spanish participation in cyber exercises</td>
</tr>
<tr>
<td>No. international cyber exercises with Spanish participation</td>
<td>Spanish participation in international cyber exercises</td>
</tr>
<tr>
<td>No. cyber exercises that involve the public sector</td>
<td>Participation of public sector in cyber exercises</td>
</tr>
<tr>
<td>No. cyber exercises that involve the private sector</td>
<td>Participation of private sector in cyber exercises</td>
</tr>
<tr>
<td>No. editions hold/year</td>
<td>Temporal evolution of cyber exercises</td>
</tr>
<tr>
<td>No. cyber tabletop exercises</td>
<td>Scenarios for cyber exercises</td>
</tr>
<tr>
<td>No. full-scale cyber exercises</td>
<td></td>
</tr>
<tr>
<td>No. cyber exercises that cover every phase of the incident</td>
<td></td>
</tr>
<tr>
<td>No. cyber exercises that cover the first phase of the incident (before)</td>
<td>Cyber exercises scope regarding the incident phases</td>
</tr>
<tr>
<td>No. cyber exercises that cover the second phase of the incident (during)</td>
<td></td>
</tr>
<tr>
<td>No. cyber that cover the third phase of the incident (after)</td>
<td></td>
</tr>
<tr>
<td>No. cyber exercises with just one edition</td>
<td>Regularity of cyber exercises</td>
</tr>
<tr>
<td>No. cyber exercises with more than one edition</td>
<td></td>
</tr>
<tr>
<td>No. cyber exercises included in the Digital Agenda for Europe</td>
<td>Inclusion of cyber exercises in the Digital Agenda for Europe implementation</td>
</tr>
</tbody>
</table>

### 3.4 CYBER EXERCISES PROFILING

After applying the above metrics to information gathering on cyber exercises, results have been obtained, which allow a profiling of the cyber exercises as detailed below.

#### 3.4.1 Participation of countries in cyber exercises

The number of participant countries in cyber exercises at global, international, and national levels, has been taken into account. The cooperation between countries is highlighted by this aspect.
Global level means the total number of cyber exercises that have been conducted; international level: cyber exercises involving more than one country; national level: cyber exercises organized within a single country.

- Participant countries in cyber exercises

The number of participating countries in cyber exercises was analyzed, distinguishing those that involved only a country, against those with up to 20, or more than 20 countries.

As shown in the graph, most cyber exercises have been national (73%), versus international cyber exercises (27%). This is mainly due to the maturity of the cyber exercises over time, so that the first occasions are held within a country, and do not involve more countries until it is reached a certain level of maturity.

![Participant countries](image)

**Figure 3. Participant countries**

- EU participant countries in cyber exercises

The participation of EU countries in cyber exercises is analyzed, and as it is shown in the following figure, EU countries have participated in more than half of all exercises identified.
The assessment of the participation of EU member states in international cyber exercises, defined as those involving more than one country, was considered of interest. The EU countries have participated in more than half of world class cyber exercises analyzed that involves more than one nation. This indicates an active participation of EU countries at internationally level.
The percentage of cyber exercises with participation of the EU member states have been analyzed, being useful to assess how many international cyber exercises have had a large share of those Member States.

For this purpose, the following graph represents the percentage of international cyber exercises that have benefited from the joint participation of several EU member states, distinguishing between those cyber exercises in which until 20 EU member states participate together, and those in which this share exceeds 20 countries. The conclusion is that about 16% of international cyber exercises have relied on the joint participation of up to 20 EU countries, and more than 20 EU countries have jointly participated in only 7% of international cyber exercises.

This analysis shows the high participation of EU countries in international cyber exercises, which is aligned with the trend of cyber exercises enhancing their degree of internationalization, looking forward to increasing the number of participating countries.
Figure 6. Cyber exercises that involve joint participation of EU countries

Figure 7. Countries involved in international cyber exercises per year
• Number of cyber exercises with Spanish participation

Spain participates in 21 cyber exercises, 11 of which are international, and the rest are national cyber exercises.

It is observed the cooperation and coordination of Spain with the surrounding countries, either European or NATO.

![Number of cyber exercises with Spanish participation](image)

*Figure 8. Number of cyber exercises with Spanish participation*
3.4.2 Sectors Involved

One interesting point to analyse is the involvement of participants in the exercises belonging to different vertical sectors, as well as the involvement of the public and/or private sectors.

Vertical sectors include the various strategic areas defined by the Law 8/2011 on measures for the protection of critical infrastructure, that is:

- Transport.
- Energy.
- Financial.
- Water.
- Health.
- ICT (Information and Communication Technologies).
- Chemical.
- Nuclear.
- R&D.
- Food.
- Space.
- Public Administration.

**Vertical Sectors involved in cyber exercises**

It was found that, as expected in exercises dealing with ICT, the most involved sector is the ICT sector which was identified in 27 cyber exercises, followed by Financial, Transport and Energy sectors.

**Figure 10. Vertical Sectors involved in the cyber exercises**

**Vertical Sectors jointly involved in cyber exercises**

In addition to analyzing the number of cyber exercises that are involved in each of the sectors described above, it has been considered of interest to identify those cyber exercises involving various sectors together. Thus, those cyber exercises involving a single sector have been differentiated compared to those involving three or more vertical sectors.
Figure 11. Cyber exercises involving different Vertical Sectors

- Public and private sectors involved in cyber exercises

Similarly, the involvement of public and private sectors have been analyzed. Cyber exercises may involve both types, so that the results in the chart below do not necessarily add up to 100%.

It has been found that 95% of cyber exercises involve public sector, compared to 50% involving private sector; 45% of cyber exercises involve both of them.

Even though public and private sectors did not initially participate together in cyber exercises, now it has become a standard and even desirable practice. The single involvement of public sector usually responds to the need to initiate or enhance national capacities related to cyber security, before involving private sector. It may also respond to the fact that scope of the cyber exercises adheres to the military environment.
3.4.3 Cyber exercises modality

Considering how cyber exercises are performed, they may belong to a different modality.

Some are called *tabletop*, which consist of discussions of hypothetical scenarios in an informal setting, with the aim of evaluating the plans, policies and procedures, and systems necessary for the prevention, response and recovery of a particular incident.

Another modality of cyber exercises are called *full-scale*. These cyber exercises are more complex since they involve multiple organizations and jurisdictions, in order to validate many aspects, such as implementing and analysing the plans, policies, procedures and cooperative agreements developed in discussion-based exercises.

The graph below shows information regarding *tabletop* or *full-scale* cyber exercises, which are the only types that have been identified in the *information gathering*, having been explicitly reported.

From the information gathered, it can be concluded that 35% of cyber exercises analysed perform exercises with *tabletop* modality, compared to 6% of cyber exercises that perform exercises with *full-scale* modality. The ease of implementation and lower
The cost of tabletop cyber exercises may be the main reason why they are the most used. Since each cyber exercise realization can run different modalities of exercises, the aggregate of the percentages do not have to correspond to 100.

![Modality of cyber exercises](image)

Figure 13. Modality of cyber exercises

### 3.4.4 Time Pattern of cyber exercises

- **Number of cyber exercises per year**

Regarding the number of cyber exercises held over time, we observe a clear increase of the number of cyber exercises in recent years, reaching 26 held in 2012, the most prolific year. However, a slight decrease is also observed in the last two years. The causes of this decline have not been analysed in depth in this paper, although it should be noted that the present study has been carried out without completing year 2014, and has been based largely on information available on the implementation of the Digital Agenda and ENISA report, both in 2012.
Figure 14. Number of cyber exercises per year

- Regularity of cyber exercises

Concerning the regularity of cyber exercises those who were held only once have been identified, against those who have had several editions over years, with a regularity in time.

The conclusion is that 49% of cyber exercises have been held more than once, and regularly. This indicates a commitment to continuity, with the consequent improvement process for each new cyber exercise in time and also probably one of the causes of "preserving" the cyber exercise is because the threat or object remains valid.
3.4.5 Cyber exercises included in the Digital Agenda for Europe

Knowing the exercises that are included in the implementation of the Digital Agenda for Europe, provides information about which are significant for each of the member countries. From this analysis, it should be noted that over 80% of cyber exercises analysed are not included in the Digital Agenda for Europe.
3.4.6 Indecent phases covered by cyber exercises
Cyber exercises can be focused in one or more phases of a possible incident: before, during or after the incident occurs. It has been considered important to identify which phases have been covered in cyber exercises, concluding that all phases are covered only in the 20% of cyber exercises, while most cyber exercises focus only on the time of occurrence of the incident (55%). It should be noted that a cyber exercise can cover several phases, therefore being represented in more than one phases from the graph below, so that the total is not necessarily 100%.

Figure 16. Cyber exercises included in the Digital Agenda for Europe
This aspect highlights the performance of the US, which is the country that most often includes all phases of the incident in its cyber exercises.

3.4.7 Participation level of EU countries in international cyber exercises

The following figure provides some examples about the level of participation of the EU member states in international cyber exercises, which involve more than one country. A distinction between those countries that have a high involvement in international cyber exercises (such as Estonia, Germany and Austria), versus those with a medium participation (such as Italy, Spain or France) has been established.

For example, it is remarkable the German participation in both, international cyber exercises organized by European countries and those organized by other countries such as the US (Cyber Storm III) or the Asian region (Drill APCERT 2014).
4 CYBER EXERCISES: PROPOSED TAXONOMY

The proposed taxonomy has been developed according to the previous analysis and profiling of existing cyber exercises, and taking into consideration the studies carried out.
by two organizations of different geographical influence like ENISA y APEC\textsuperscript{7}. The taxonomy consists of the five basic elements depicted in the next figure:

1. **Focus**
   This element presents what the cyber exercises if focused in, regarding its evaluation goal, purpose and phase of the incident that is covered (for instance awareness, improve, etc.) and try to assess what aspects (plans, procedures, etc.) and which phases of the incident are covered (occurring before, during or after the incident).

2. **Model**
   This element presents the different type of cyber exercises, depending on whether they are discussion based (for instance *tabletop, game* or *workshop*), or operational based (for instance *full simulation* or *drill*).

3. **Vertical Sector**
   This element includes the sectors involved in the cyber exercise, according to the strategic sectors defined in the Spanish law 8/2011\textsuperscript{8} \textsuperscript{9}, which establishes critical infrastructures protection measures.

4. **Participation Scope**
   This element presents the participants origin, according to their geographical provenance, public or private sector involvement, and the role they play within the cyber exercise.

\textsuperscript{7} \url{http://www.mtc.gob.pe/portal/apectel38/spsg/08_tel38_spsg_013_APEC_Draft_Exercise_Report%5B1%5D.pdf}

\textsuperscript{8} \url{http://www.boe.es/buscar/doc.php?id=BOE-A-2011-7630}

\textsuperscript{9} \url{http://www.boe.es/diaro_boe/txt.php?id=BOE-A-2011-8849}
5. Results Dissemination

This element comprehends the level of dissemination applied to the results of the cyber exercise, regarding if they are accessible or private.

Next figure presents every field of the proposed taxonomy, which will be described in sections below.

![Figure 20. Taxonomy Schema.](image)

4.1 FOCUS

The focus of the cyber exercise contains three main goals, which are the purpose of the incident, the evaluation objective and the phase of the incident that is covered by the cyber exercise.
• **Purpose**

The purpose of a cyber exercise can be: to raise awareness between participants, to initiate or establish the implementation of certain tasks or actions within the organization, or to improve already implemented actions.

• **Evaluation**

Cyber exercises are commonly aimed at evaluating specific tasks or actions within the organization, which apply at different phases of an incident life cycle. This tasks can be evaluated in terms of policies (involving nations, organizations, information exchange, security, etc.), agreements (collaboration, cooperation, mutual help, etc.), plans (like recovery plans), procedures (like Security Operating Procedures), processes (like evaluating the efficiently within the organization) or capabilities (like the skills of the participants).

• **Incident Phase**

Cyber exercises may cover different phases of the incident life cycle. Theses phases include the previous phase before the incident takes places, the phase when the incident occurs, or the phase after the incident has happened.

### 4.2 MODEL

From the models proposed by ENISA, the *tabletop* and *full-scale* models covered a large group of cyber exercises that had been identified (62%), while 22% of cyber exercises matched the model "other" cyber exercise. However, upon review of the specification models of APEC, it has been found that they can fit both models defined by ENISA (the...
ones with the same name is trivial lace, and other models fit as specific performance of drills), and the various editions of cyber exercises that have been collected.

Figure 22. Model Element.

- **Discussion Based**
  These types are used as the first exercises to be performed within an organization, to gradually increase the complexity. This model of cyber exercises typically focus on strategic issues, allowing to familiarize with current or planned capacities, either plans, policies, agreements or procedures. This model of cyber exercise includes different modalities such as seminars, workshops, tabletop and games.

  a. **Seminar**
     Seminars are informal discussions that provide an overview to participants. They are a starting point for developing or making major changes to the organization plans and procedures.

  b. **Workshop**
     Workshops focus on the most effective achievement or development of a particular outcome. The more specific, the more effective they will be.

  c. **Tabletop**
     Tabletop consist of discussions among key people about hypothetical scenarios in an informal setting, with the aim of evaluating the plans, policies and procedures, or the systems needed to address the phases of an incident.

  d. **Game**
     Games describe a real or alleged situation. The goal is to explore the process of decision-making and its consequences, without using real resources.
• **Operations Based**

These types are used to validate the plans, policies, agreements and procedures, which have been consolidated in discussion based cyber exercises. This model enables to clarify roles and responsibilities, identify gaps in implementing plans and procedures, and improve individual and collective performance. This model includes different modalities such as drills, functional and full-scale cyber exercises.

a. **Drill**

Drills are often used to validate a transaction or a specific function in a particular organization. They are commonly used for team building, to develop or test new policies or procedures, or to practice and maintain current skills.

b. **Functional**

Functional cyber exercises are designed to validate and evaluate individual capabilities, as well as to test plans, policies, procedures and staff of an organization. This modality of exercise stimulates the operations in a functional area, by presenting complex and real problems that require quick and effective responses in a stressful environment with time constraints.

c. **Full-scale**

This modality of cyber exercise is the most complex. Full-scale cyber exercises often focus on the implementation and analysis of plans, policies, procedures and cooperative agreements developed in discussion based exercises, and improved in previous years based on smaller operations. The level of support and funding necessary to perform this modality of exercise is greater than any other exercise.

4.3 **VERTICAL SECTOR**

There have been considered the different strategic vertical sectors defined in the Law 8/2011 on the establishment of measures to protect critical infrastructures. The ICT sector has been the most involved in cyber exercises.
4.4 SCOPE FOR PARTICIPATION

This element is aimed at outlining the participation of individuals in the cyber exercises, for it takes into account sectorial affiliation (public or private), geographical location and the role played within the organization.

Figure 23. Vertical Sector Element.
4.5 DISSEMINATION OF RESULTS
Regarding the dissemination of results, it has been shown that there is a segregation of information disseminated both to general public and private public (such as certain groups of participants or to each participant individually).
5 TAXONOMY APPLICATION IN CYBER EXERCISES

Once the taxonomy is developed, a number of relevant cyber exercises is selected from the gathering set, to obtain an example of the characterization thereof.

5.1 SELECTION OF CYBER EXERCISES

The selection of exercises cyber is mainly due to the results obtained by applying the previously defined metrics.

A relevant sample of cyber exercises, that were held recently, have been selected. The used criteria include only recent cyber exercises that:

- They are at national level located in Spain.
- Spain is on the participants, and they are contained in the implementation of the Digital Agenda for Europe.

For the remaining cyber exercises, that were not selected with the previous criteria, the following criteria have been applied to:

- Those that are held on a regular basis over time, and full scale modality is present
- They are focused on one specific vertical sector (finance or health), and preferably with the participation of European countries.
The list of the latest editions of cyber exercises that have been relevant after applying the selection criteria are:

<table>
<thead>
<tr>
<th>EXERCISE</th>
<th>YEAR</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYBER STORM</td>
<td>2013</td>
</tr>
<tr>
<td>LOCKED SHIELDS</td>
<td>2014</td>
</tr>
<tr>
<td>CYBER COALITION</td>
<td>2014</td>
</tr>
<tr>
<td>CYBERATLANTIC</td>
<td>2011</td>
</tr>
<tr>
<td>CYBEREUROPE</td>
<td>2014</td>
</tr>
<tr>
<td>EUROCYBEX</td>
<td>2011</td>
</tr>
<tr>
<td>EUROSOPLEX</td>
<td>2012</td>
</tr>
<tr>
<td>CYBER-EX</td>
<td>2013</td>
</tr>
<tr>
<td>PSCIC</td>
<td>2014</td>
</tr>
<tr>
<td>EJERCICIO DE CIBERDEFENSA</td>
<td>2014</td>
</tr>
<tr>
<td>CYBERRX</td>
<td>2014</td>
</tr>
<tr>
<td>WAKING SHARK</td>
<td>2013</td>
</tr>
</tbody>
</table>

Table 5. List of cyber exercises considered as relevant

### 5.2 APPLICATION OF TAXONOMY

The following figures show the application of the taxonomy to the previous selection:

![Figure 26. Taxonomy Schema for Cyber Storm 2013.](image)
Figure 27. Taxonomy Schema for Locked Shields 2014.

Figure 28. Taxonomy Schema for Cyber Coalition 2014.
Figure 29. Taxonomy Schema for CyberAtlantic 2011.

Figure 30. Taxonomy Schema for CyberEurope 2014.
Figure 31. Taxonomy Schema for Eurocybex 2011.

Figure 32 Taxonomy Schema for EuroSopex 2012.
Figure 33. Taxonomy Schema for Cyber-Ex 2013.

Figure 34. Taxonomy Schema for PSCIC 2014.
Figure 35. Taxonomy Schema for ECD 2014.

Figure 36. Taxonomy Schema for CyberRx 2014.
Applying the taxonomy to relevant cyber exercises using criteria specified in the previous section, allows to establish an implementation map of cyber exercises according to various characterizations discussed in the following subsections.

### 5.2.1 Sectorial Perspective

While ICT is present and affect all strategic sectors, only specific cyber exercises of ICT vertical sector has been considered in the analysis when it faced directly as an essential service provided by ICT operators or had their participation. This decision was taken to maintain consistency with the strategic sectors identified by the Law 8/2011 of Spain.

Therefore, from a sectorial perspective, a specific characterization has not been made for a cyber exercise when it does not specifically facing a specific vertical sector.

The following figure shows again the number of times the vertical sectors have been involved in the cyber exercises conducted.
As can be seen there are many exercises that address cyber vertical sectors of Transport and Energy. Both sectors are identified in the European Directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

The ICT sector is also specifically addressed in the cyber exercises very often sector that is identified in the European Directive as the next area of application in future revisions of the Directive.

The financial crisis has an impact on the rise of cyber exercises in the financial sector, highlighting the number of cyber exercises conducted that has seen the sector.

However, it has not found any cyber exercise that takes into account the area of R & D despite the importance of this sector in times of crisis to give added value to the economy of each country.

Cyber exercises focused on the space sector were not found, despite the dependence on multiple sectors with services that provided. However, in a working paper of the European Commission where a new approach to software protection of European critical infrastructures is addressed, four specific infrastructures of European dimension are selected, one of them being Galileo, the European program for global satellite
navigation system. Therefore it is assumed that cyber exercises including the space sector is carried out in the near future, and more specifically Galileo.

The remaining sectors have a low representation in the cyber exercises conducted, which suggest some concern from those sectors but might need the right impetus, either by regulators or by news that requires protecting certain services with some urgency. For instance, in line with the latter, the recent cases of pandemics could generate social demand in the protection of the health services that are supported by ICT systems.

5.2.2 Used Models
The models used in cyber exercises are very different according to whether they are based on discussions, or in operations or even a mixture of both. The greatest number of cyber exercises are based on discussions; not surprising since they are the ones usually begins before developing an operational capacity and usually require less resources in their preparation.

The following figure shows the percentage of occurrence of exercise models in the cyber exercises conducted, although it should be noted that some cyber exercises may contain several exercises of the same model, so the sum of percentages does not correspond to 100%.

![Cyber exercises models](image)

*Figure 39. Cyber exercises Models*

Different scenarios have been identified based on the models of cyber exercises which are reproduced in the following table:
<table>
<thead>
<tr>
<th>MODEL OF CYBER EXERCISES</th>
<th>SCENARIOS</th>
</tr>
</thead>
<tbody>
<tr>
<td>DISCUSSION BASED</td>
<td>TABLETOP</td>
</tr>
<tr>
<td></td>
<td>TABLETOP + SEMINAR</td>
</tr>
<tr>
<td></td>
<td>TABLETOP + SEMINAR + WORKSHOP</td>
</tr>
<tr>
<td></td>
<td>GAME</td>
</tr>
<tr>
<td></td>
<td>TABLETOP + GAME</td>
</tr>
<tr>
<td>OPERATIONS BASED</td>
<td>DRILL</td>
</tr>
<tr>
<td></td>
<td>FULL-SCALE</td>
</tr>
<tr>
<td></td>
<td>FUNCTIONAL</td>
</tr>
<tr>
<td></td>
<td>FUNCTIONAL + FULL-SCALE</td>
</tr>
<tr>
<td>MIX</td>
<td>TABLETOP + FULL-SCALE</td>
</tr>
</tbody>
</table>

*Table 6. Scenarios used regarding the model of cyber exercises*

The following figure represents the percentage of occurrence of each model patterns in cyber exercises. As in the previous figure, the occurrence of each modality of cyber exercise is depicted, so that the aggregate of the percentages do not have to correspond to 100.

Most of the cyber exercises performed are tabletop, game or drill. But maybe many seminars and workshops have not been counted as cyber exercises.
The exercises, regardless of their modality, are usually performed to evaluate certain tasks or activities within an organization that have application in any phase of an incident, as a policy, agreement, plan, procedure, process or a given capacity.

The following figure shows the percentages of occurrence of the various aspects evaluated in the cyber exercises performed on total thereof, several evaluation aspects by exercise may appear, so that the aggregate of the percentages do not have to sum 100. Noteworthy is the high degree of occurrence that have the capacity, because many exercises seek staff training.
The purpose of the cyber exercise, could be to raise awareness, to start/set some tasks or activities within an organization, or to improve some tasks or activities within an organization. The following figure represents the percentages of occurrence of the different objectives pursued in the conducted cyber exercises on total thereof, several purposes by exercise may appear, so that the aggregate of the percentages do not have to sum 100. It should be noted the purpose of improvement, as the most frequent appearance, because many exercises seek the improvement of the evaluated target.
The cyber exercise can be focused on the phase of pre-incident, phase of during the incident and after the incident. Also can cover several phases.

The following figure shows the appearance according to the covered phase of incident in the conducted cyber exercises and may be several per exercise. The aggregate of the percentages therefore do not have to sum to 100.

The main area of activity of the exercises is corresponding to the incident response, i.e., the phase during the incident is the most displayed one. If the cyber exercise is performed in conjunction with an exercise in crisis management, involving emergency services, the phase after the incident is usually addressed.
5.2.3 Situation in Spain

Spain has participated in several cyber exercises, that have been organized in Europe with the support of the European Commission and also those, as allied country, has been organized by NATO. This ensures that the cooperation and coordination of Spain with the rest of the neighbouring countries, so it is guaranteed either by the European side or by the Atlantic alliance side. The following figure shows the number of cyber exercises with the participation of Spain.
In cyber exercises organized by the US (Cyber Storm) is frequent involving European countries like Germany, Holland, France and the UK, but Spain has not participated in these exercises.

On the other hand, Germany has been the only country member of the European group of governmental CERTs (EGC) to participate in a cyber exercise in the Asia-Pacific region organized by the APCERT. Spain as a member of EGC could participate in future editions of those exercises.

From a local perspective, Spain has organized several cyber exercises both in the military and civilian matters. While the cyber exercises focused on vertical sector suffer from the operations based model, it is assumed that the near future will be conducted despite the enormous effort that is necessary to use resources both in its preparation and execution, given the results obtained.

For vertical sectors covered in Spain, the only striking variation from all the exercises is the lack of involvement of the financial sector in them.
Continuing with the national level, Spain has not conducted a joint exercise of overall crisis management that includes the cyber aspect, as for example it has been conducted by Germany or NATO.

6 CONCLUSIONS

The European momentum through the Digital Agenda for conducting cyber exercises, has achieved that most of the member states participate in pan-European cyber exercises, and even perform their own national cyber exercises.

It has been noted that many countries assume the global, complex and increasingly sophisticated nature of threats in cyberspace, being necessary to address these threats in cooperation with other countries. In this regard, it has been found different scenarios where European countries:

1. Perform a national exercise in a timely manner, although they also participated in European ones.
2. Perform national and European exercises independently, without coordinating the implementation of one another.
3. Intend to synchronize their national exercises with European ones, so that they are conducted in a parallel manner.
4. Actively participate in international exercises, not just European ones.

Although public and private sectors did not participate together in cyber exercises initially, now it has become a standard and even desirable practice. The single involvement of public sector usually responds to the need to initiate or enhance national capacities related to cyber security, before involving private sector. It may also respond to the fact that scope of the cyber exercises adheres to the military environment.

High participation of European countries in international cyber exercises is remarkable, it has been aligned with the trend of cyber exercises enhancing their degree of internationalization, looking forward to increasing the number of participating countries.

Most of the cyber exercises are tabletop, games or drills. Nevertheless, it is possible that many seminars and workshops have not been counted as cyber exercises.

Although the purpose of a cyber exercise may consider many aspects, different approaches, both collective and individual, have lived together seamlessly in various editions.

Many cyber exercises are structured to be hold in different stages of implementation, each one of them focusing on a different role within each organization. In this respect, a common thread to perform such cyber exercises can be found, but they could also be considered as separate exercises.
Public results dissemination is increasingly meagre, inferring the private dissemination of results to each participant.

While countries like the US focus their cyber exercises in covering all phases of the cyber incident, the need to cover the recovery phase when planning new cyber exercises has been raised.

Many of the cyber exercises are performed regularly, on an annual or biannual basis. This gives the opportunity to validate cyber exercises improvement, as well as the training of its participants. However, the evolution of threats and technology hinders the capacity for improvement, since it requires evaluate other aspects.

Cyber exercises are increasingly involving new vertical sectors, being the US the pioneer country in organizing such exercises just for one sector such as financial or health. Thus being stated the dependency of those vertical sectors on ICT.

Regarding vertical sectors involved in cyber exercises is been found that:

- There is a high involvement of vertical sectors such as transport, energy and ICT.
- It is common to take into account sectorial interdependencies when matched several vertical sectors in the same cyber exercise.
- There is no evidence of cyber exercises involving R & D or Space sectors.
- There is a need to encourage the rest of vertical sectors.

Regarding Spanish situation, it has been observed that:

- There is cooperation and coordination with other neighbouring countries, either European or NATO.
- It would be appropriate to participate in transatlantic cyber exercises.
- It is necessary to promote national cyber operations based exercises.
- There is minor involvement of financial sector compared to other cyber exercises conducted by other countries.
- It would be necessary to conduct a joint overall crisis management exercise, which includes cybernetics.
7 LISTS and REFERENCES

7.1 LIST OF FIGURES

Figure 1. Methodology ........................................................................................................... 7
Figure 2. Methodology for information gathering and analysis of cyber exercises .......... 9
Figure 3. Participant countries ............................................................................................... 15
Figure 4. Participant EU countries in cyber exercises ......................................................... 16
Figure 5. Participant EU countries in international cyber exercises .................................... 17
Figure 6. Cyber exercises that involve joint participation of EU countries ....................... 18
Figure 7. Countries involved in international cyber exercises per year ............................. 18
Figure 8. Number of cyber exercises with Spanish participation ....................................... 19
Figure 9. Number of cyber exercises with Spanish participation per year ....................... 20
Figure 10. Vertical Sectors involved in the cyber exercises ................................................ 21
Figure 11. Cyber exercises involving different Vertical Sectors .......................................... 22
Figure 12. Public and Private sectors involved ................................................................. 23
Figure 13. Modality of cyber exercises ................................................................................ 24
Figure 14. Number of cyber exercises per year .................................................................. 25
Figure 15. Regularity of cyber exercises ........................................................................... 26
Figure 16. Cyber exercises included in the Digital Agenda for Europe ............................. 27
Figure 17. Phases of the incident covered by the cyber exercises ...................................... 28
Figure 18. Participation level of EU members in international cyber exercises ............... 29
Figure 19. Basic Taxonomy Elements ............................................................................... 30
Figure 20. Taxonomy Schema ......................................................................................... 31
Figure 21. Focus Element .................................................................................................. 32
Figure 22. Model Element ................................................................................................. 33
Figure 23. Vertical Sector Element .................................................................................... 35
Figure 24. Participation Scope Element ............................................................................. 36
Figure 25. Results Dissemination Element ...................................................................... 37
Figure 26. Taxonomy Schema for Cyber Storm 2013 ...................................................... 38
Figure 27. Taxonomy Schema for Locked Shields 2014 ................................................ 39
Figure 28. Taxonomy Schema for Cyber Coalition 2014 ................................................ 39
Figure 29. Taxonomy Schema for CyberAtlantic 2011 .................................................... 40
Figure 30. Taxonomy Schema for CyberEurope 2014 ..................................................... 40
Figure 31. Taxonomy Schema for Eurocybex 2011 ......................................................... 41
Figure 32 Taxonomy Schema for EuroSopex 2012. ...............................................................41  
Figure 33. Taxonomy Schema for Cyber-Ex 2013. ..............................................................42  
Figure 34. Taxonomy Schema for PSCIC 2014. ................................................................42  
Figure 35. Taxonomy Schema for ECD 2014. ..................................................................43  
Figure 36. Taxonomy Schema for CyberRx 2014. .............................................................43  
Figure 37. Taxonomy Schema for Waking Shark 2013. ....................................................44  
Figure 38. Vertical Sectors involved in the cyber exercises..............................................45  
Figure 39. Cyber exercises Models ..................................................................................46  
Figure 40. Cyber exercises Modality..................................................................................48  
Figure 41. Cyber exercises Evaluation. ............................................................................49  
Figure 42. Cyber exercises Purpose ...............................................................................50  
Figure 43. Phases of the incident covered by the cyber exercises.....................................51  
Figure 44. Number of cyber exercises with Spanish participation.................................52

7.2 LIST OF TABLES

Table 1. Acronyms.................................................................................................................6  
Table 2. Completeness of collected information by exercise..............................................13  
Table 3. Metrics by cyber exercise and associated indicator .............................................13  
Table 4. Global metrics and associated indicators ...............................................................14  
Table 5. List of cyber exercises considered as relevant.....................................................38  
Table 6. Scenarios used regarding the model of cyber exercises.......................................47