CEIS

EUROCYBEX

Pan-European cyber-crisis exercise

Axel Dyèvre,
Guillaume Tissier
& Timothée Grange.

Light version

AFTER EXERCISE REPORT

March 2012

Euro Cybex 2011

CONFIDENTIALITY DISCLAIMER

Some sentences or paragraphs have intentionally been masked or removed for confidentiality reasons. A full version of this report has been realized and printed for Public Authorities involved. The aim is to avoid any leak about security measures and procedures.

If you think that you could be a relevant receipt for the full report, please contact
bruxelles@ceis.eu
The request will be assessed with the partners of the consortium.

EUROCYBEX This project has received funding from the European Union CIPS Programme (DG HOME). The sole responsibility lies with the authors and that the European Commission is not responsible for any use that may be made of the information contained therein.

CEIS is a strategy and risk-management Research and Consultancy Firm. Our mission is to assist our clients with their development in Europe and abroad and contribute to the protection of their interests. To that end, we systematically combine foresight and an operational approach, with control of useful information for decision support and action.

ANSSI The French Network and Information Security Agency (ANSSI), created in 2009, is the national authority for information systems defence and security in France. It is directly attached to the Head of General Secretariat for Defence and National Security, under the authority of the Prime Minister.

CERT-HUNGARY is hosted by the Theodore Puskas Foundation. It acts as the National Cyber Security Center of Hungary since 2010, being responsible for the security of the government network under the supervision of the Ministry of National Development.

CNPIC is the National Centre for Critical Infrastructure Protection in Spain, being the national coordinating authority and the international Point of Contact in the matter. We are in charge of assessing the criticality of strategic infrastructures, fostering information exchange among public and private stakeholders and putting forward all the measures needed to ensure confidentiality and to improve critical infrastructure protection.

GOVCERT AUSTRIA is the Austrian Government Computer Emergency Response Team. Its constituency consists of Austria's public administration and critical information infrastructure (CII). Founded in April 2008, this organisation is run by the Federal Chancellery in cooperation with CERT.at to handle and prevent security-relevant incidents in the area of information and communication technologies.

ISDEFE is a state owned company that offers engineering, strategic consulting, technical assistance, program management and project execution service to Spain's administration and to international organizations, especially Spanish Ministry of Defence, as well as other civil and military organisations of the European Community, NATO, and other pan-European and international public agencies. ISDEFE forms part of the structure of the Spanish Ministry of Defence, which oversees its actions.

TABLE OF CONTENTS

GLOSSARY

ANSSI - Agence Nationale de la Sécurité des Systèmes (France)
BSI - Bundesamt für Sicherheit in der Informationstechnik (Germany)
CEIS - Compagnie Européenne d'Intelligence Stratégique
CERT - Computer Emergency Response Team
CIPS - This EU funding programme contributes to the protection of citizens and critical infrastructures against terrorist attacks and other security-related incidents.
CNPIC - Centro Nacional para la Protección de las Infraestructuras Críticas (Spain)
ComCheck - Communications check
CRITIS - CRisis Integrated Training System
DG HOME - Directorate General Home Affairs (European Commission)
DG INFSO - Directorate General Information Society (European Commission)
EndEx - End of the exercise
ENISA - European Network and Information Security Agency
EU Commission - European Commission
EU Council - Council of the European Union
EXCON - Exercice control cell
ISDEFE - Ingeniería de Sistemas para la Defensa de España (Spain)
MS - Member State
MSEL - Main Scenario Event List
SOP(s) - Standard Operating Procedure(s)
StartEx - Start of the exercice

1. PRESENTATION & PLANNING OF THE PROJECT

1.1. Presentation

EuroCybex is a European project that has at its core a cyber-crisis exercise involving a number of European Member States. The aim is to test and improve the communication procedures between Member States. The project started in January 2011 and concluded by mid-2012.
EuroCybex is conducted by a consortium, led by CEIS, a Research and Consultancy firm specialised in intelligence, defence and security issues, working with EU Institutions, national governments, agencies and the private sector (www.ceis.eu).

Partners in the consortium are:

- Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI – France – www.ssi.gouv.fr)
- Centro Nacional para la Protección de las Infraestructuras Críticas (CNPIC – Spain – www.cnpic.es)
- Theodore Puskas Foundation (CERT – Hungary – www.cert-hungary.hu)
- Ministère de l'Economie, de l'Industrie et de l'emploi (MINEFI – France – www.economie.gouv.fr)
- Ingeniería de Sistemas para la Defensa de España (ISDEFE – Spain – www.isdefe.es)

At the **EuroCybex exercise conducted in September 2011**, four member states participated as players (France, Germany, Austria and Hungary), 20 others followed the exercise as observers and attended the debriefing.

The ENISA and the DG INFSO of the European Commission support the project, and they are also the members of the project advisory board.

Thanks to the members of the consortium and the advisory board, the EURO-CYBEX project has been conducted with careful attention to the calendar of official exercises at EU and international level. Drawing on lessons learned from the first pan-European cyber exercise, Cyber Europe 2010, it has also

contributed to the work on SOPs and scenario for the coming exercises, Cyber Atlantic 2011 and Cyber Europe 2012.

With a total budget of 200 000 euros, the EuroCybex project received 69 % of co-funding from DG HOME of the European Commission in the framework of the programme CIPS. This funding programme contributes to the protection of citizens and critical infrastructure against terrorist attacks and other security-related incidents.

1.2 Planning and Execution

13 January 2011

Workshop 1: **Kick-off meeting** in Brussels. The core team of the project, composed of the six partners, designed the initial version of the EuroCybex project. The key objective of the project is the following: **updating and validating the EU Standard Operating Procedures** (SOPs) for cyber-crisis.

In order to do so, a tabletop exercise using the CRITIS platform (CRisis Integrated TraIning System) will be organised by and with partners of the consortium. CRITIS is a web platform developed by CEIS, aiming to manage the exercise, to inject the events and to collect feedback for the post-exercise analysis. CRITIS, as a role-playing tool, allows each participant to log on to his own profile and to give access to a specific interface according to the role definition (see detailed presentation in part 2.5).The other member states (MS) will be invited to join the exercise as players or observers. The exercise was planned for early 2012.

28 February 2011

The decision was taken to contact **ENISA** directly (part of the Advisory Board and aware of all outputs of the project) in order to fully **integrate the EuroCybex Project in the development of EU SOPs** for cyber-crisis exercises.

14 April 2011

EU Home Affairs Commissioner, Cecilia Malmström, and Secretary of the US Department of Homeland Security, Janet Napolitano, reiterated their shared commitment to deepening cooperation to address the increasing threats to global internet and digital networks. They agreed to strengthen trans-Atlantic cooperation in cyber-security by defining the issues to be tackled by the EU-US Working Group on CyberSecurity and CyberCrime. The decision was made to improve incident management response capabilities jointly and globally, through a cooperation programme culminating in a joint EU-US

cyber-incident exercise by the end of 2011.

26 April 2011

A **working meeting** was conducted in Paris to facilitate the integration of EuroCybex in the **planning of EU cyber-crises exercises**. The group worked on the necessary actions to conduct testing and improve the standard operating procedures (SOPs) during the exercise. The decision was taken to extend the core team to several other identified countries.

4 May 2011

Workshop 2: Representatives of four more member states (MS) and representatives from ENISA and from DG INFSO joined the meeting. The project, and its objective,were presented and discussed. The EU SOPs were also presented and several potential improvements were highlighted. The CRITIS platform was demonstrated and several ideas were proposed to improve the realism of the scenario and the exercise. The issue of the forthcoming EU-US exercise was discussed but no agenda was available to measure the potential impact on the agenda of EuroCybex. Following this meeting, two member states, **Germany and Austria, decided to join the exercise as players**, that is, members of the "core team".

27 May 2011

Meeting was held between the **national cyber-agencies and ENISA** regarding the planning of cyberexercises before the end of 2011. Due to the EU exercise now fixed for end of October 2011, the national cyber-agencies and ENISA decided to ask CEIS to organise the EuroCybex exercise in September 2011 in order to **test the SOPs** before the EU-US exercise. After consultation with CEIS and with the partners, the decision was made to organise the EuroCybex exercise in **September 2011**. A new workshop had to be organised very quickly to fix the framework of the exercise.

22 June 2011

Workshop 3 in Brussels: the two new playing MS and ENISA decided to plan the exercise, and fix the next steps of the project jointly with the partners of the consortium. The exercise was planned for **27 September 2011**, and details of the scenario and progress of operations up to this date were detailed. The partners agreed to dedicate the necessary resources, which were initially planned for use over a longer timeframe. All partners agreed to this change.

End of June 2011 – mid-September 2011

Numerous **telephone conferences and small informal meetings** between the enlarged core team, including Germany and Austria, were organised

over this period to coordinate the work done, and to set up the exercise on time. All relevant organisations in member states have been contacted by the ENISA to check if they were interested in following the exercise.

During this period, the **inputs on the Main Scenario Event List (MSEL)** were committed by the participants in coordination between members (events, press events, etc). Several **tele-training sessions** were also organised for players and observers in order to train them in the use of the CRITIS platform. In the last two weeks before the exercise itself, several **assessments** were organised with the core team reviewing the progress.

27 September 2011

The **EuroCybex exercise took place from 10.00 am to 15.00 pm, involving nearly 50 people**. Four participating MS played, using the CRITIS platform and observed by more than 30 representatives of EU and MS institutions. At the end of the session, an online survey was sent to all using a secure system provided by CEIS. Seventeen forms were filled in, most of them are submitted by country – thereby representing several participants.

28 September 2011

A hotwash session was organised with representatives of the entities that filled in the evaluation form. The aim was to debrief on the early results from the forms and to **complete the questionnaire** with a discussion on key issues and lessons learned.

7 November 2011

- **Dissemination event:** In the framework of the "**Security & Defence Day**", organised under the Patronage of the Polish Presidency of the EU Council (www.secdef.eu), there was a **session on cyber issues** in partnership with the EuroCybex Project. More than **300 people attended the conference and more than 50 attended the session where EuroCybex was presented**. A presentation of the project is also included in the programme and the website of the conference.
- **Dissemination**: in the framework of the conference, a "special edition" of the EU journal "Europolitics" was published. An **article presenting the project** and its lessons learned is published in this edition. A "**presentation page**" about the project is also included (about 5 000 readers + the electronic version).
- Dissemination: the **report on the conference** includes the "presentation page" and the report of the sessions in partnership with EuroCybex.

October 2011 – February 2012

Writing of the present **report and related annexes**.

2. SCENARIO & EXERCISE EXECUTION

2.1 General theme of the scenario*

National cyber defence agencies try to assess, respond and contain the crisis. The media are already aware of the situation. Some journalists have been contacted by the attackers. Nonetheless, no press article on the matter has been released before the start of the exercise. At this stage no international cooperation has been initiated yet.

Considering this information, participating countries are likely to conclude they were probably attacked by the same group and should try to cooperate to best mitigate the crisis.

The scenario of EuroCybex was developed to enhance communication procedures between MS and to come up with, test and improve SOPs.

2.2 Exercise set-up

Exercise type: distributed through a virtual exercise control cell. The participants used their usual communication means from their office or crisis rooms. There was no need for moderators in a centralised exercise control cell (CEIS hosted a virtual exercise control room).

Level of participation: crisis managers / operations directors.

Exercise preparation: moderators have organised a meeting with their participants to present the objectives of the exercise and to share the relevant documents. This presentation was conducted before the communications check (ComCheck).(13 Sept. 2011).

Date of the exercise: 27 September 2011 from 10.00 a.m. CET to 2.21 p.m. CET.

Participants: Four MS playing (**Austria, France, Germany, Hungary**); 13 observers.

*Some paragraphs have intentionally been removed for confidentiality reasons.

2.3 Participation

The statistics below have been created by crossing the exercise directory and the CRITIS access logs in order to take into account only effective participation.

2.3.1 Number of participants

In total, **41 people have been directly involved in EuroCybex** (players, national moderators or observers).

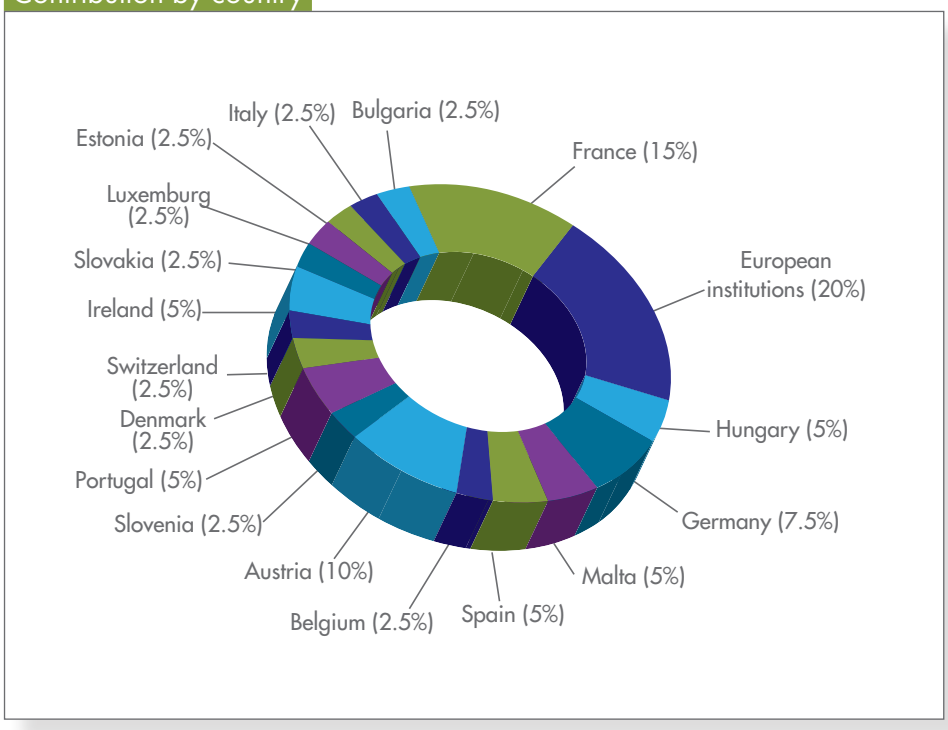
These statistics do not include the four members of the exercice control cell (EXCON) in charge of the animation of the exercise.

2.3.2 Distribution by country

The European institutions (EU Commission and affiliated organisations, EU Council) represent 20 % of the participants. They are followed by France (15 %), Austria (10 %), Germany (7,5 %), Hungary (5 %), Malta (5 %), Spain (5 %), Portugal (5 %) and Ireland (5 %).

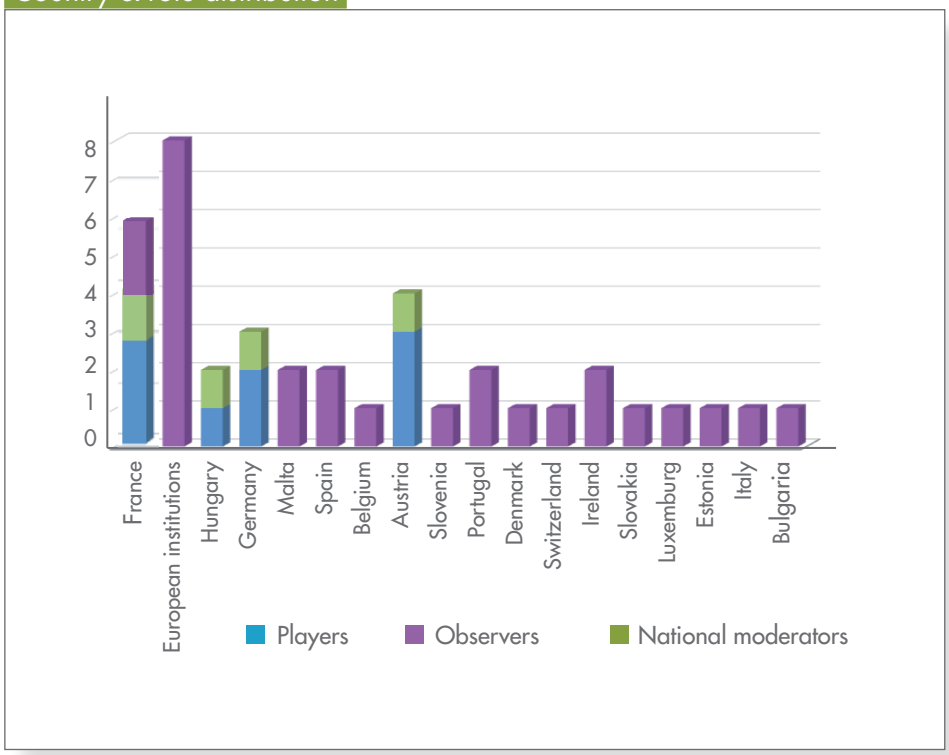
These statistics do not include the members of the EXCON.

Contribution by country



2.3.3 Distribution by country and role

Country & role distribution



2.4 Main Scenario Event List (MSEL)

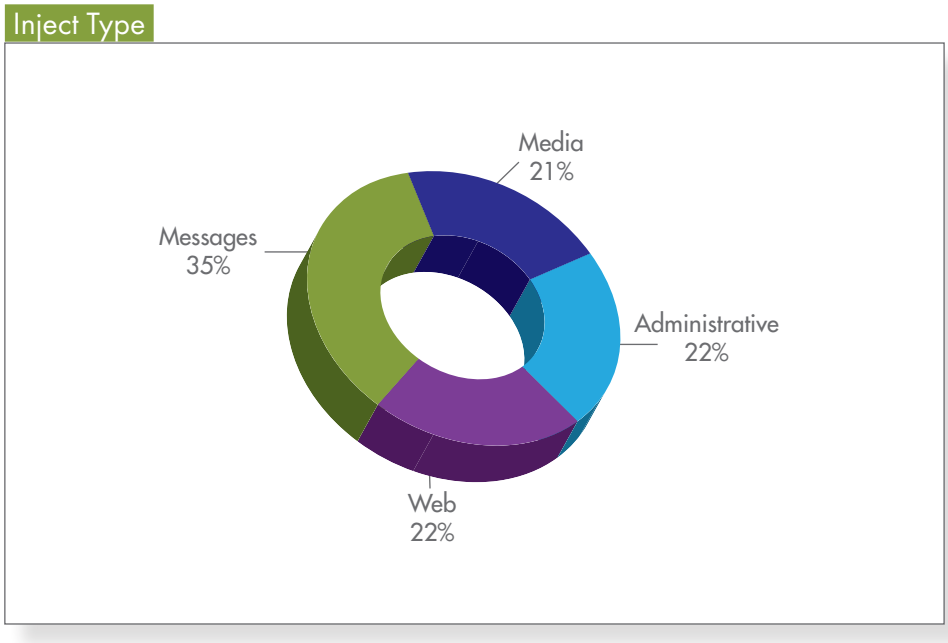
The Main Scenario Event List (MSEL) contained the substance of the scenario and was administered by the EXCON/moderators in order to manage the exercise. All injects had predefined 'senders', 'recipients', 'subject', 'type' and a scheduled publishing time. The exercise coordination and communication platform was structured around a portal named CRisis Integrated Training System (CRITIS) (Cf. chapter 2.5) that automatically provided the MS-moderators with the injected events in a timely fashion and according to the MSEL. (Cf. annexe3).

The scenario was based on **various types of inputs**: media (news articles, wire agencies), web (website new publications), simulated messages (demands from various administration), administrative messages from the exercise control cell.

2.4.1 Number of injects

Twenty-three injects were sent by the EXCON during the exercise. Some were published through the CRITIS user interface (media, web). Others were sent by email to national moderators who were asked to forward them to their players.

2.4.2 Distribution by type

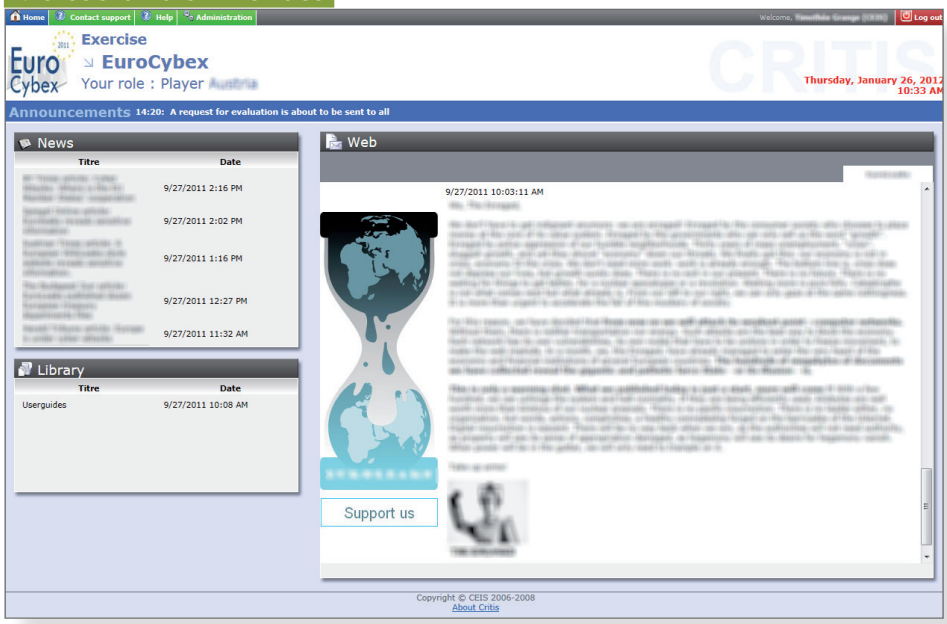


2.5 CRITIS: the exercise web platform

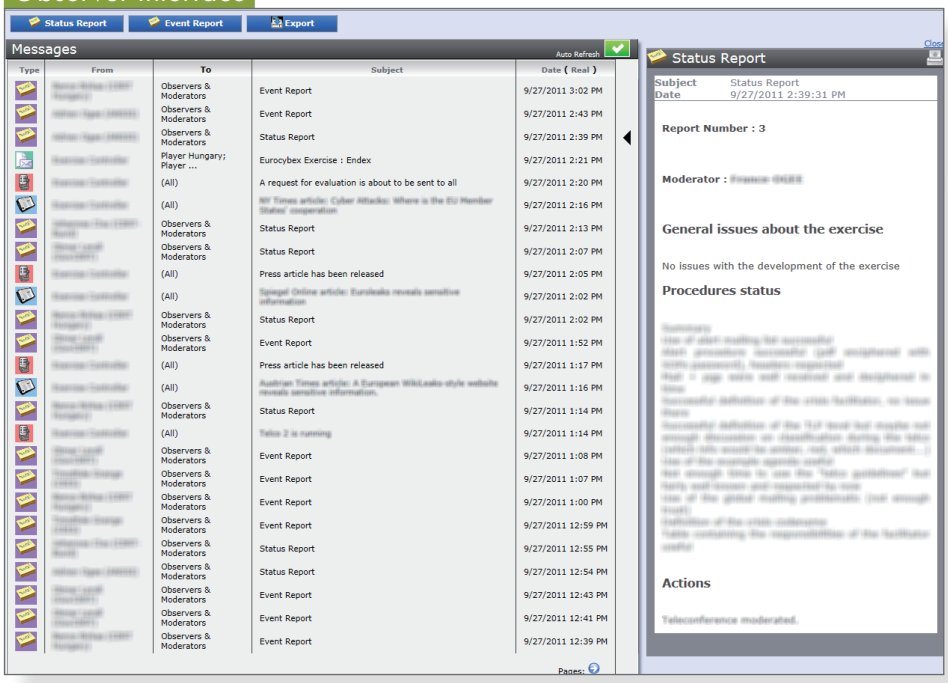
The EXCON used a **web platform called CRITIS** in order to manage the exercise, to inject the events and to collect feedback for the post-exercise analysis. CRITIS, as a role-playing tool, allows each participant to log on to his own profile and to give access to a specific interface according to the role definition. As a result, on the one hand, MS coordinators had access to their dedicated interface where they were able to receive all injects sent by the EXCON (press releases, messages, web inputs, EXCON messages) and to report these inputs to their MS players. On the other hand, observers had access to a completely different interface, where they were able to see the MSEL and the logbook. The logbook provided a detailed list of all injects created by the EXCON, and of all the inputs (status reports and events re-

ports) that MS moderators had created to report MS players' actions and reactions to stimuli.

MS coordinator Interface

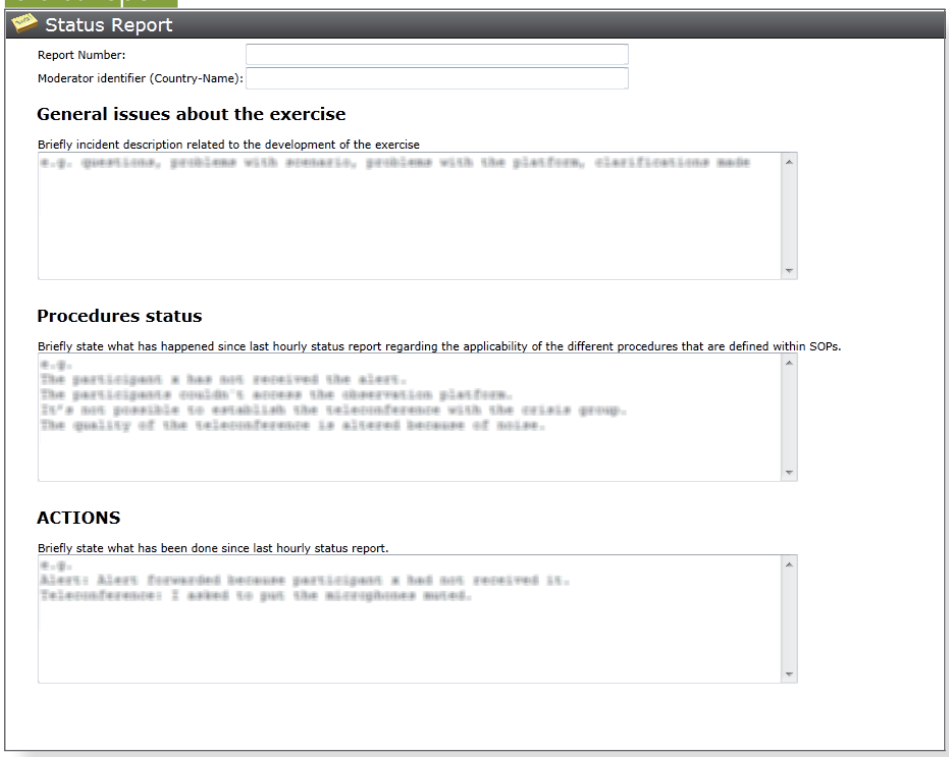


Observer Interface



Every hour, the MS moderators filled in a **status report**, covering three main subjects: issues regarding exercise flow, issues concerning the SOPs, and of course, the actions taken by the players. In addition to these status reports, MS moderators also had the opportunity to fill in event reports in case they wanted to report specific information at any time. Forty-four status and event reports were sent during the exercise by the national moderators in order to allow the EXCON cell and observers to follow the exercise.

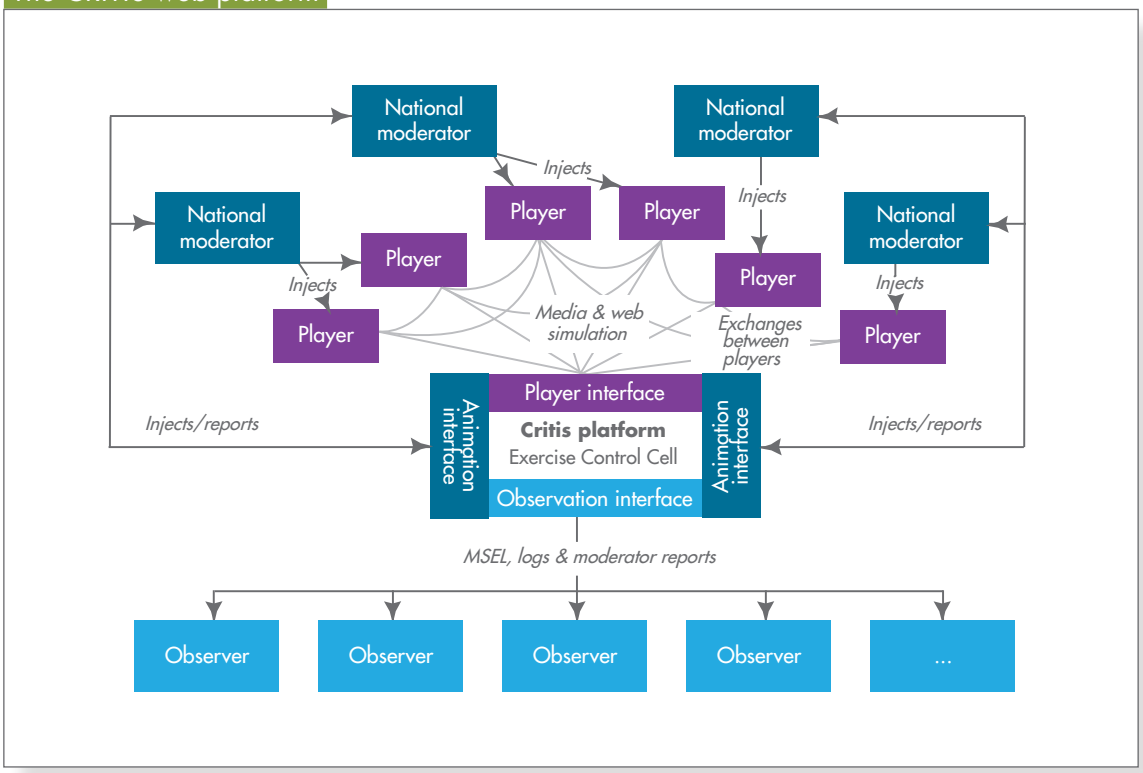
Status report



2.6 Information flows

As mentioned previously, the CRITIS web platform allows all participants to be **connected simultaneously and to exchange information** at any time during the exercise.

The CRITIS web platform



In order to get the necessary feedback for the post-exercise analysis, two types of bottom-up flows were set up:

- From national players to MS moderators:
  - Emails exchanged between players from different countries were sent in copy to the MS moderator to be entered into a national feedback database,
  - Emails exchanged between players from the same country were sent in copy to the MS moderator to be entered into a national feedback database,
  - Periodical reports were sent by each national player according to existing crisis management processes or processes to set up for the exercise. This kind of report is the only way to record phone calls between players.

- From MS moderator to Exercise moderator:
    - In order to allow the exercise moderator to check that the events were correctly sent by the MS Moderator to their national players, injected events were sent in copy to the exercise moderator,
    - Each MS moderator was asked to send reports about the actions and decisions taken by his/her national players to the exercise moderator on a regular basis. To facilitate exploitation, these reports used a specific form (date, time, name, decision taken, effects).

2.7 Scenario walk-through

10.00 a.m. (CET) **StartEx***

From 10.00 am to 11.00 am: Several **injects** were sent to simulate media pressure and phone calls from journalists. Participants attempted to define a communication strategy and started exchanges.

10.30 am: Crisis facilitator designated.

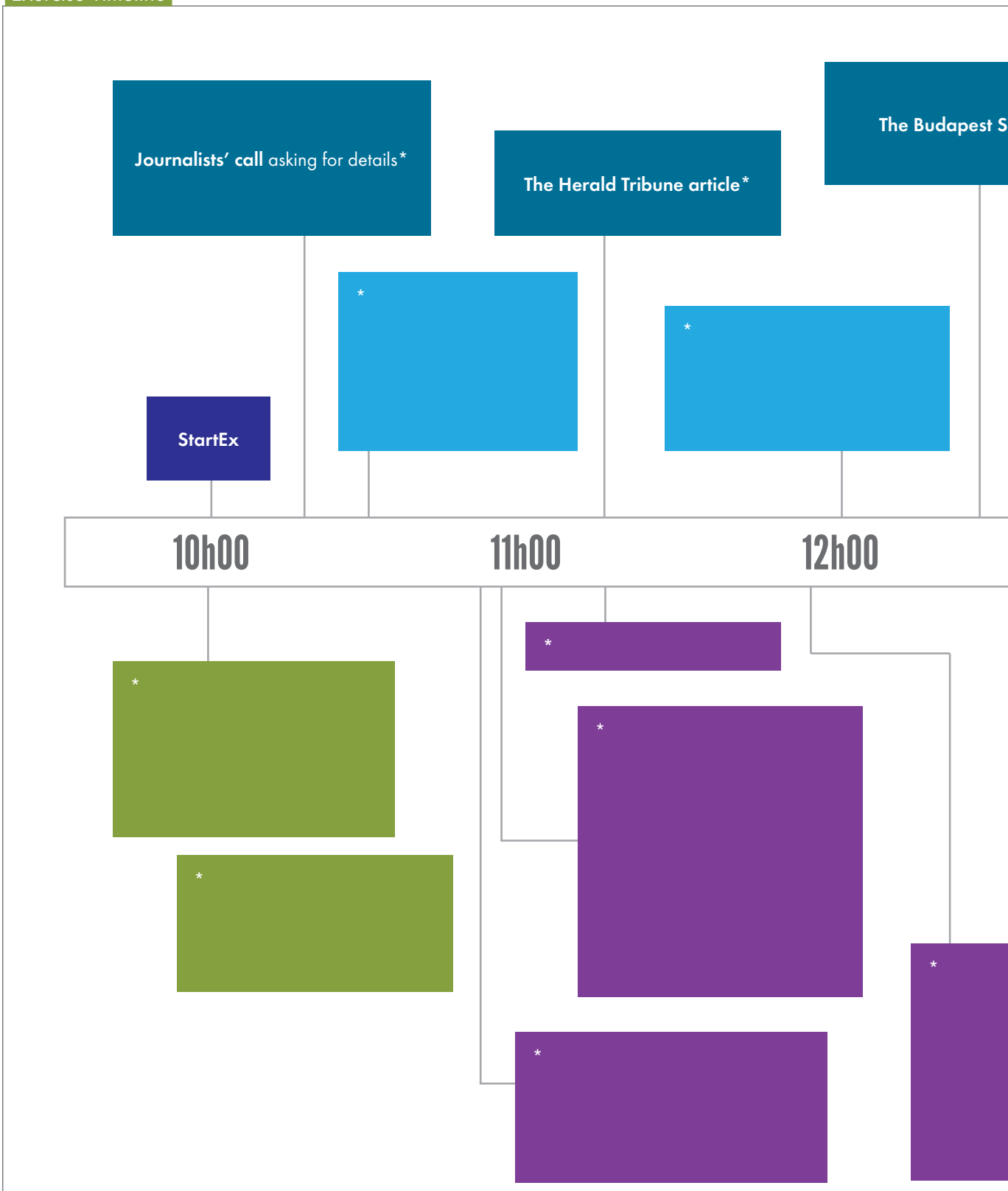
From 12.00 pm to 1 pm: **Injects** continued to simulate media pressure.

1.15 pm: MS players reached the important phase of sharing details about the attack.

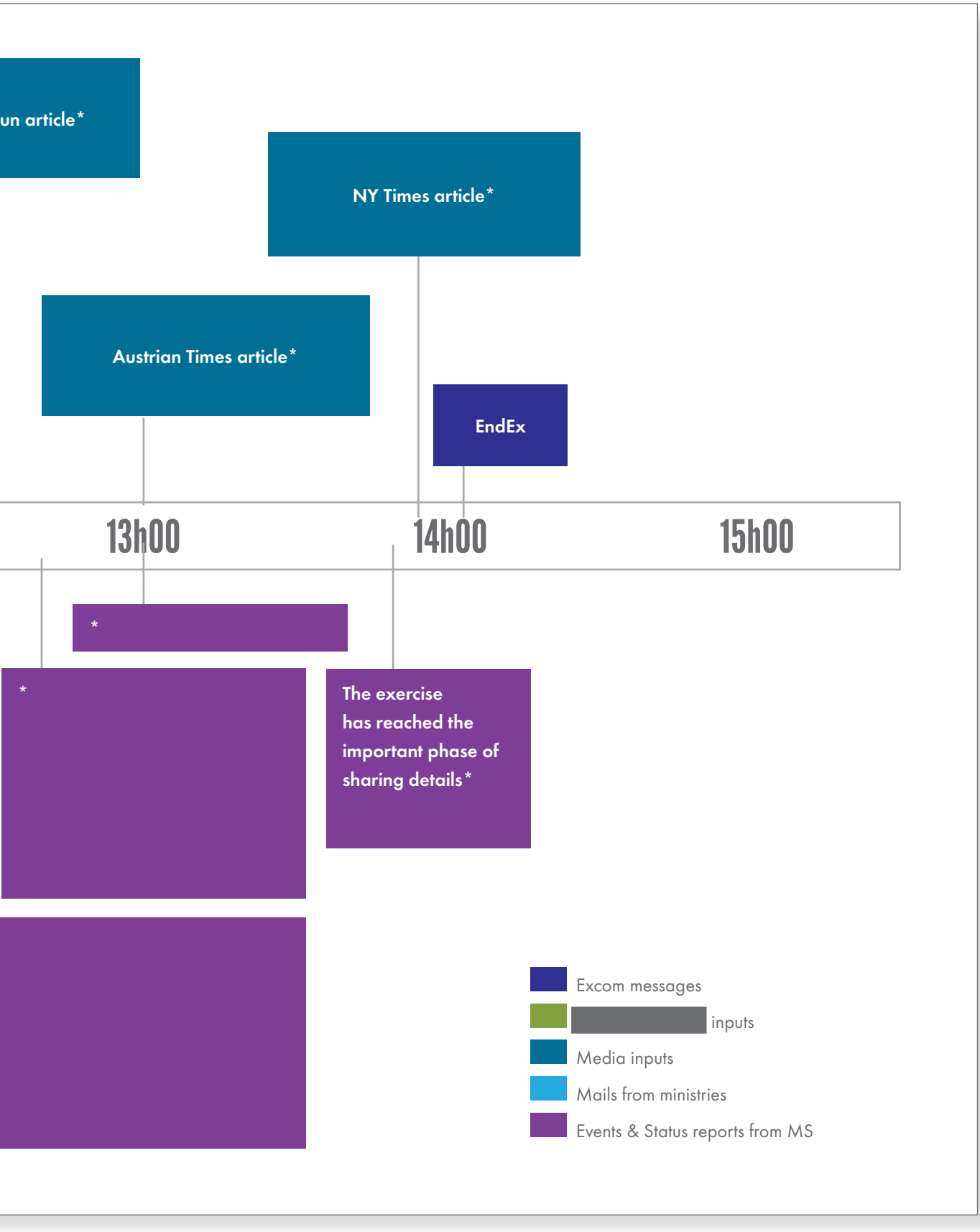
2.21 pm: **EndEx**.

*Some paragraphs have intentionally been removed for confidentiality reasons.

Exercise Timeline



*Some paragraphs have intentionally been removed for confidentiality reasons.


un article*
NY Times article*
Austrian Times article*
EndEx
13h00
14h00
15h00
*
*
The exercise has reached the important phase of sharing details*
Excom messages
inputs
Media inputs
Mails from ministries
Events & Status reports from MS

3. LESSONS LEARNED & RECOMMENDATIONS

The objective of this chapter is to analyse how participants, be they players, observers or national moderators, evaluate the exercise and the SOPs.

The data below have been collected through:

- An **electronic questionnaire** sent by email to participants, all categories included. Seventeen countries or organisations have filled it in.

Evaluation Report

Eurocybex Final Evaluation Report

1. Identification

1-1 Do you want your report to be anonymous?
Yes
No

If no, answer to the following questions.

1-2 Your firstname

1-3 Your name

1-4 Your organization

1-5 Your country

2. Lessons-learnt on the SOPs

2-1 Evaluate the alert procedure and its implementation (1: unsatisfactory 2: poor 3: satisfactory 4: good 5: excellent)
1
2
3
4
5

2-2 Comments on the alert procedure and its implementation

2-3 Evaluate the encryption scheme proposed and its implementation (1: unsatisfactory 2: poor 3: satisfactory 4: good 5: excellent)
1
2

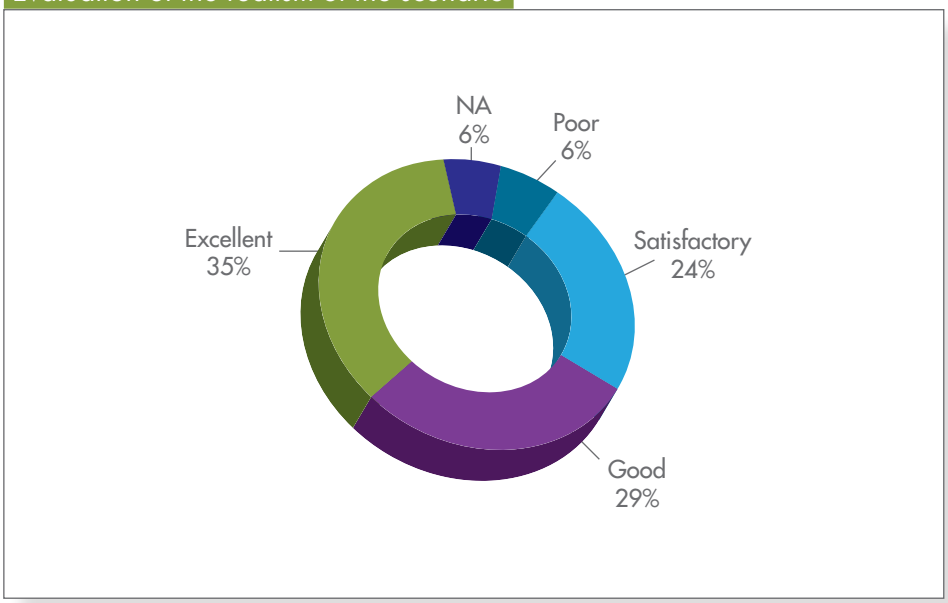
- A **hotwash** [redacted] organised with players, observers and national moderators, a few hours after the exercise.

3.1 Lessons learned on the exercise

3.1.1 Realism of the scenario

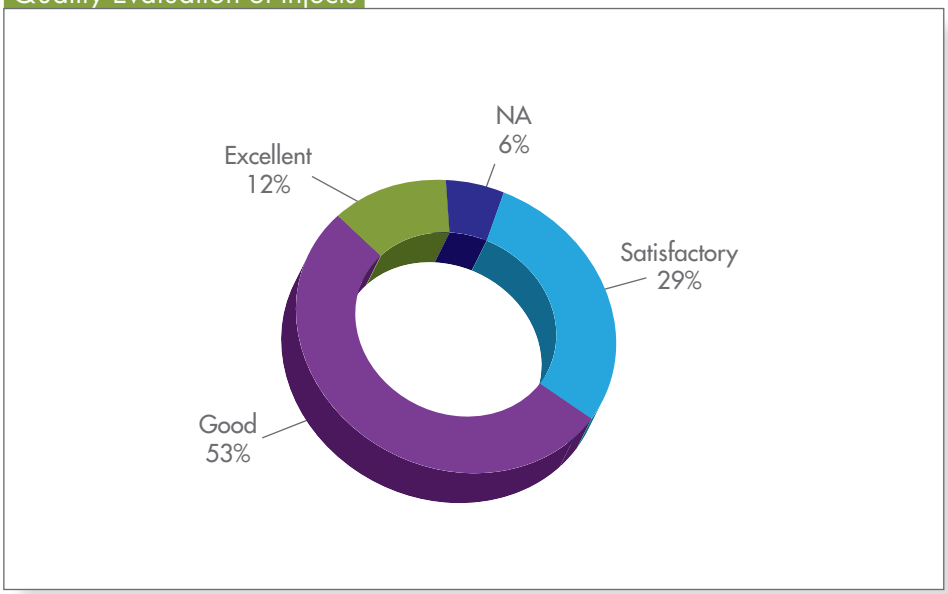
The realism of the EuroCybex scenario is considered as satisfactory, good or excellent, by **more than 80 %** of the participants. An interesting point highlighted by participants was the broad nature of the scenario framework, which can be modified by each national moderator in order to adapt it to their local context.

Evaluation of the realism of the scenario



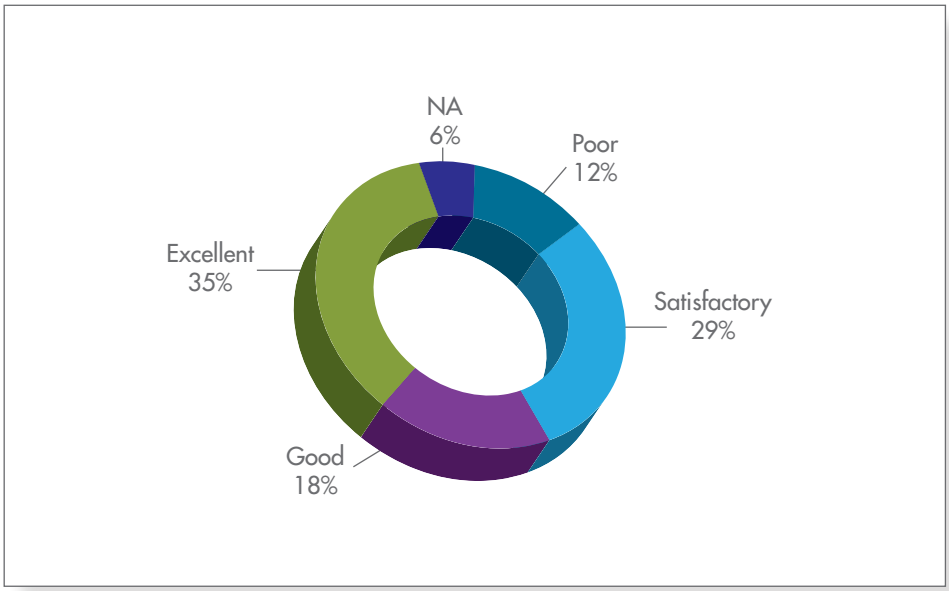
3.1.2 Quality of the Injects

Quality Evaluation of injects



Almost **65 % of the participants** considered injects as "good" or "excellent".

3.1.3 Pre-exercise briefings



Around **70 % of the participants** considered the pre-exercise briefing as "satisfactory", "good" or "excellent".

3.1.4 Logistical means and organisation

The logistical means used for the exercise were evaluated as "satisfactory", "good" or "excellent"to **nearly 90 %**. At the organisational level, attendees were particularly satisfied by the presence of each national moderator in the same room as his players.

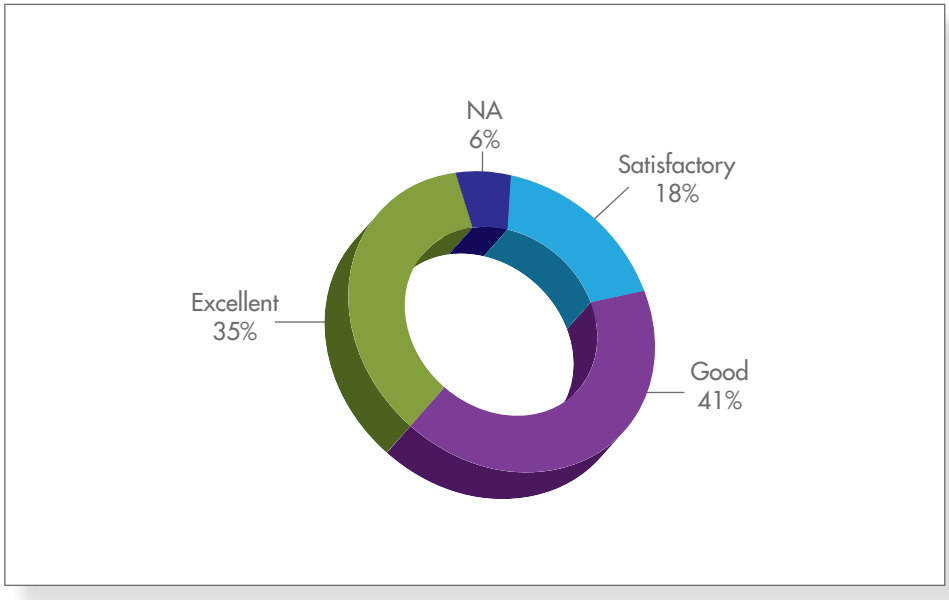
The CRITIS portal used either by players, moderators and observers was appreciated due to its user-friendly interface and its capacity to publish accurate information (MSEL, hourly and status reports) for the different categories of attendants.

Among the minor issues observed during the exercise:

*

Some minor error messages or refresh problem on the CRITIS platform (due to specific configurations of browsers).

Evaluation of logistical means

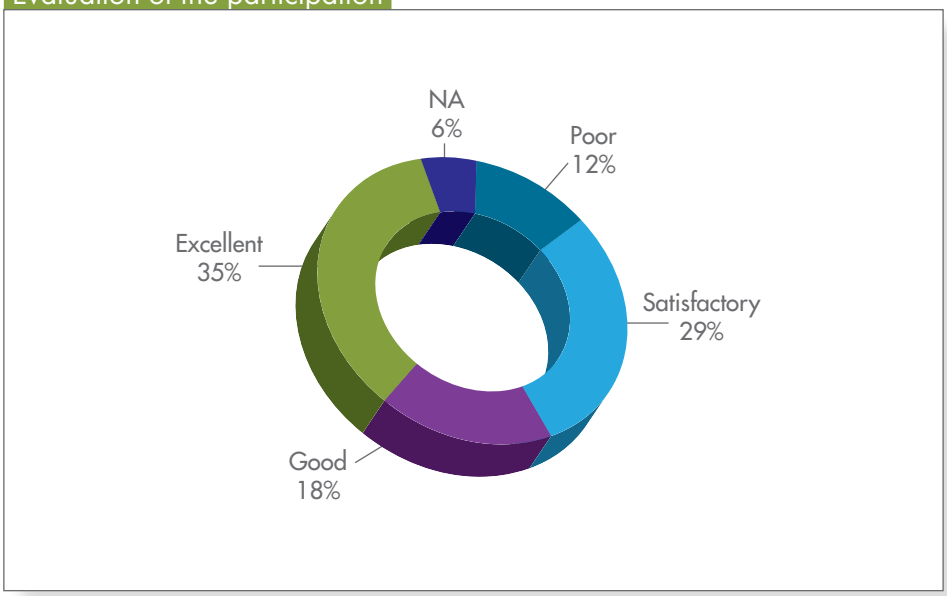


*Some paragraphs have intentionally been removed for confidentiality reasons.

3.1.5 Participation

The level of participation and involvement of attendants in the EuroCybex exercise is considered as positive by the **majority of attendees**. Some have, however, noticed that the number of participating countries (four) was too small, even if this is not necessarily a drawback for testing the SOP process.
* For each participating country, the number of organisations involved was also perceived as too limited.

Evaluation of the participation

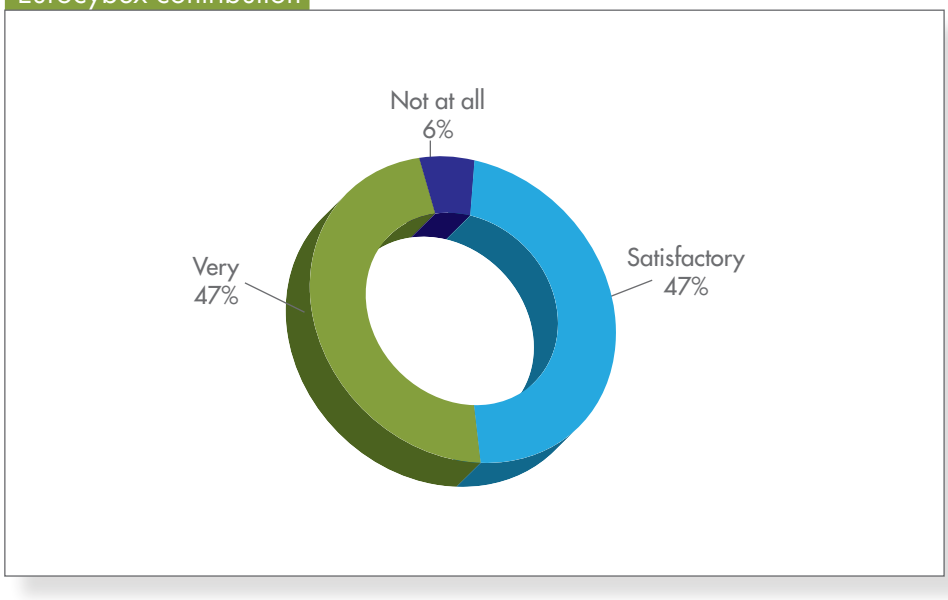


*Some paragraphs have intentionally been removed for confidentiality reasons.

3.1.6 Exercise contribution

More than **90 %** of the participants think that the EuroCybex exercise leads, at least partly, to an increased understanding on how cyber incidents could be handled within European cooperation framework.

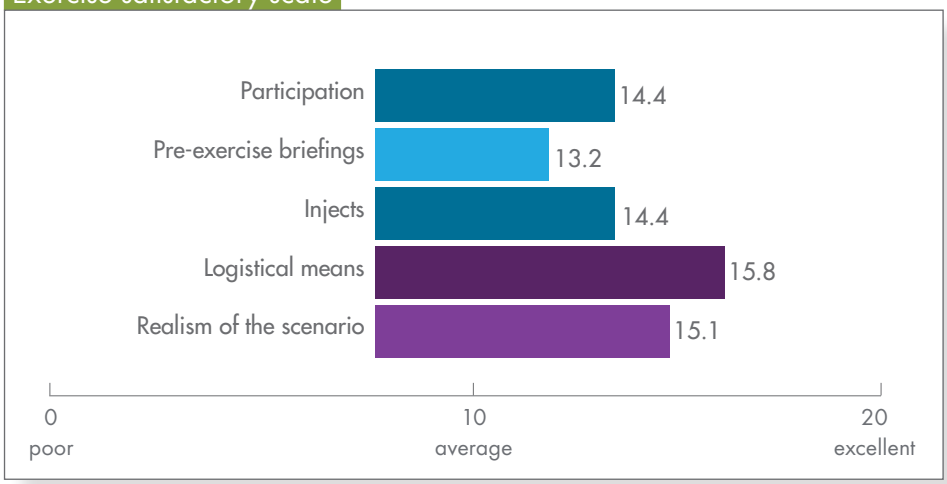
Eurocybex contribution



On a global scale, **76.5 %** of the attendees agree that European cyber exercises **help establish trusted relationship channels within Europe**, allowing for improvement of the effectiveness of public authorities in critical infrastructure information protection.

3.2 Recommendations as a result of the exercise

Exercise satisfactory scale



3.2.1 Participation

Future exercices **should involve more playing countries**. From each country, **more players** should be mobilized.

3.2.2 Scenario and injects

In order to be more realistic, **most of the injects and pre-exercise materials should be customized**. This should occur at a national level, conducted by the moderators, according to a framework provided by the animation team.

3.2.3 Logistical means and organisation

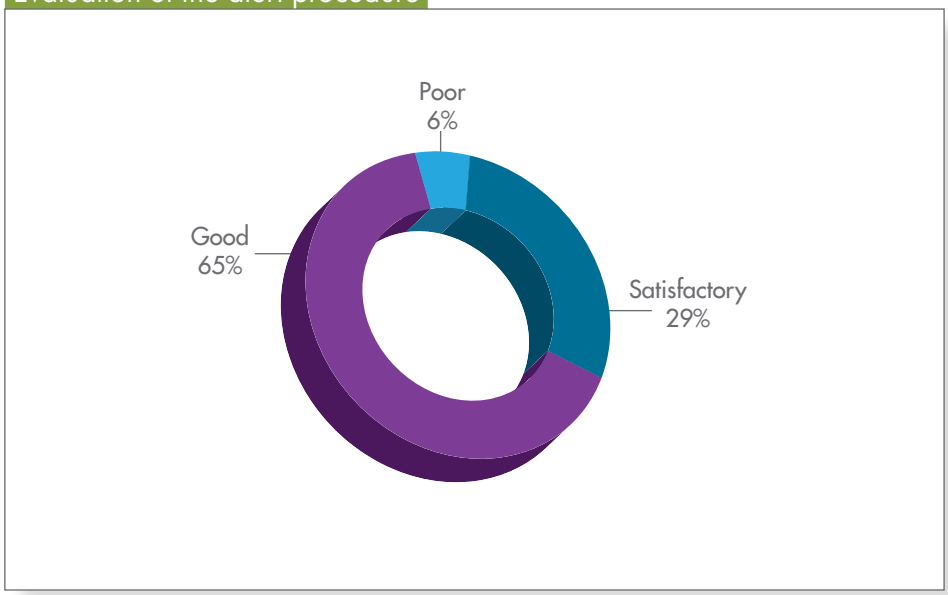
All emails exchanged between players should be sent to the Excon cell and then published on the observer interface. This would enhance the understanding and the analysis capability of the observers.

Considering that national moderators were located near their respective players, the **use of a chat system would also have been very helpful** to better coordinate the animation. Indeed, one may wonder if CRITIS could be considered more as an authentic crisis management tool, rather than as a mere exercise animation tool.

3.3 Lessons learned on SOPs

3.3.1 Alert procedure

Evaluation of the alert procedure

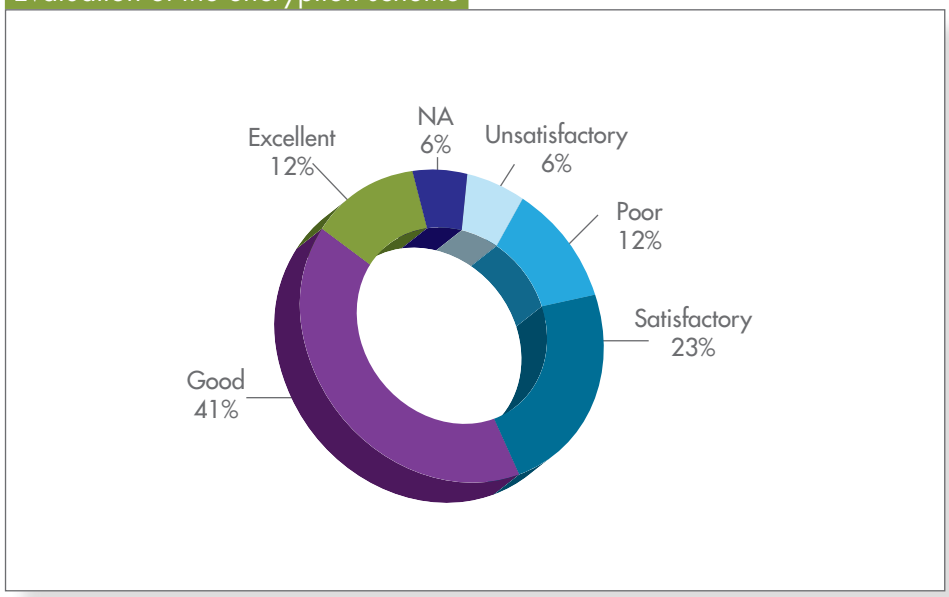


According to participants, the **alert mechanism worked well** between the four countries.*

3.3.2 Encryption scheme

*

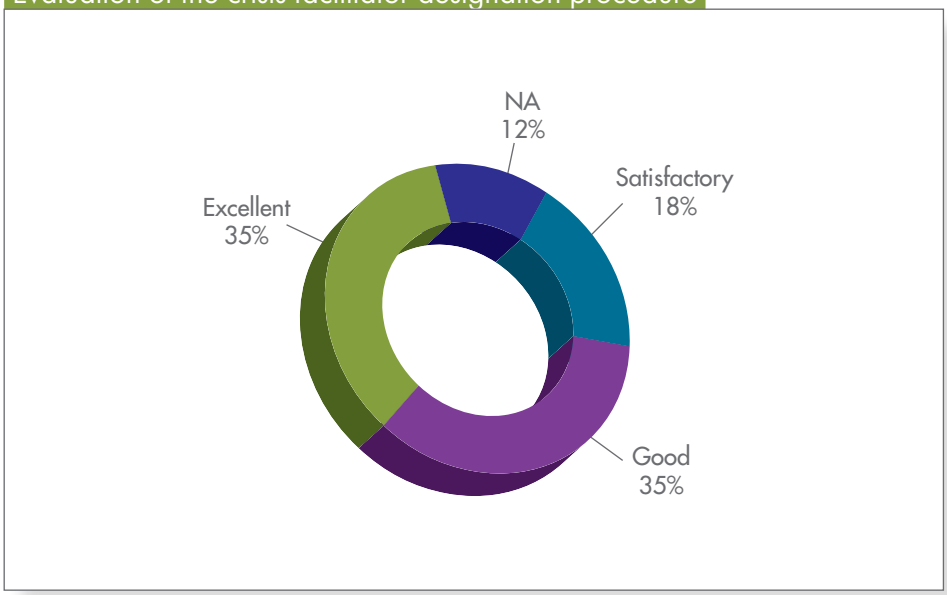
Evaluation of the encryption scheme



*Some paragraphs have intentionally been removed for confidentiality reasons.

3.3.3 Crisis facilitator designation procedure

Evaluation of the crisis facilitator designation procedure

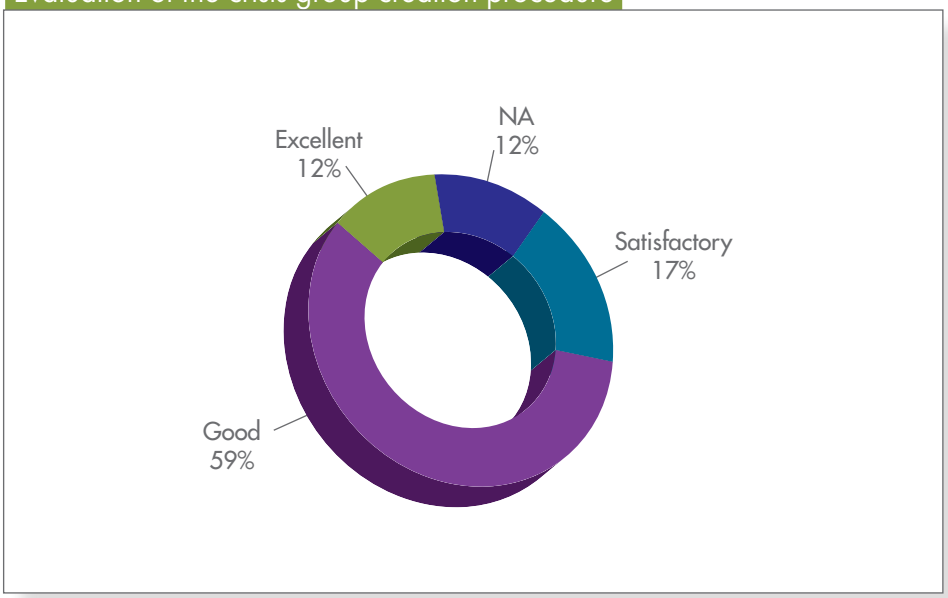


Participants considered that the **procedure for the designation of the crisis facilitator went smoothly** during the exercise, even if the players were more satisfied than the observers. The facilitator concept seemed to be appreciated by the players. *

3.3.4 Crisis group creation procedure

*

Evaluation of the crisis group creation procedure

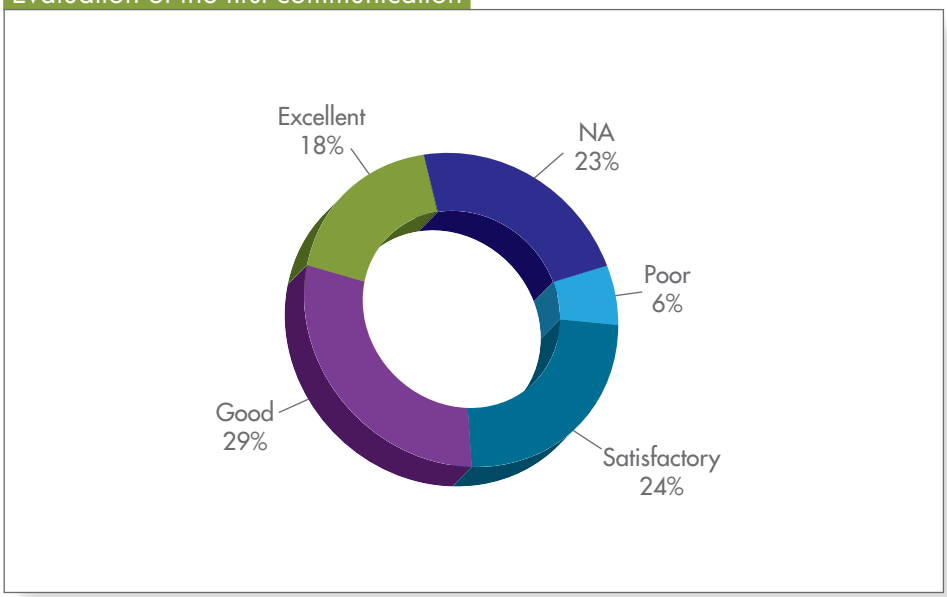


*Some paragraphs have intentionally been removed for confidentiality reasons.

3.3.5 First crisis communication

*

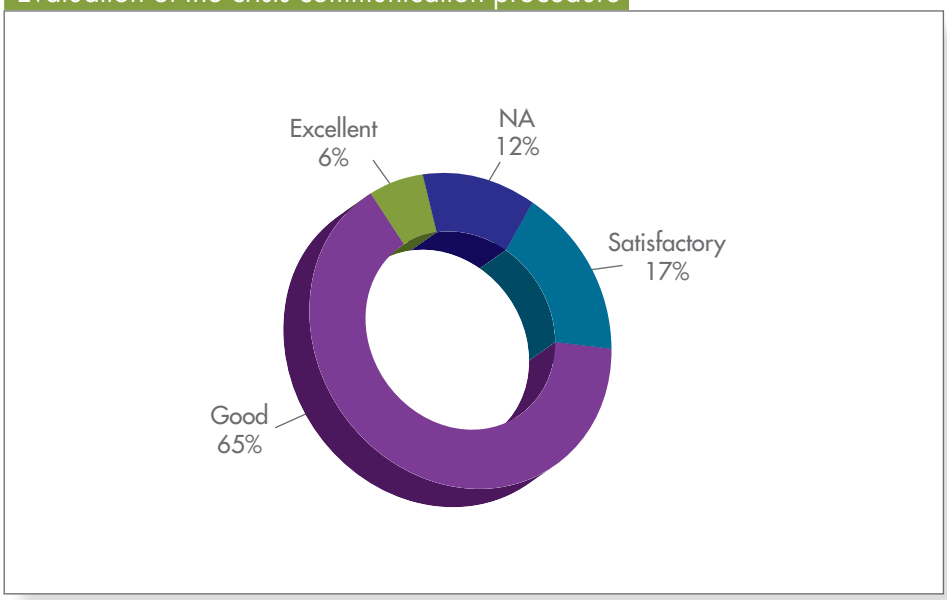
Evaluation of the first communication



3.3.6 Crisis communication procedure

88% of participants evaluated the crisis communication as "satisfactory", "good" or "excellent". According to participants this was partly due to the pre-existing trust between MS. *

Evaluation of the crisis communication procedure

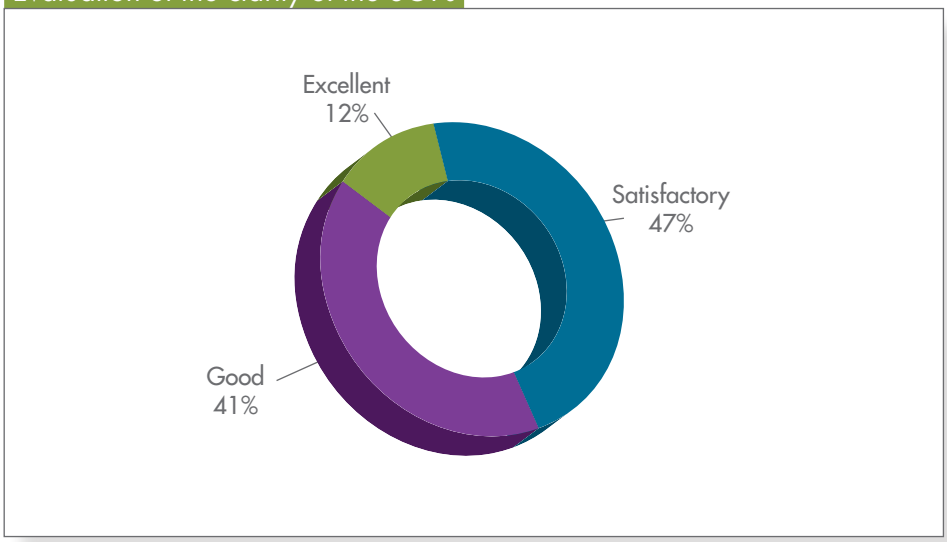


*Some paragraphs have intentionally been removed for confidentiality reasons.

3.3.7 Clarity, applicability and general comments on SOPs

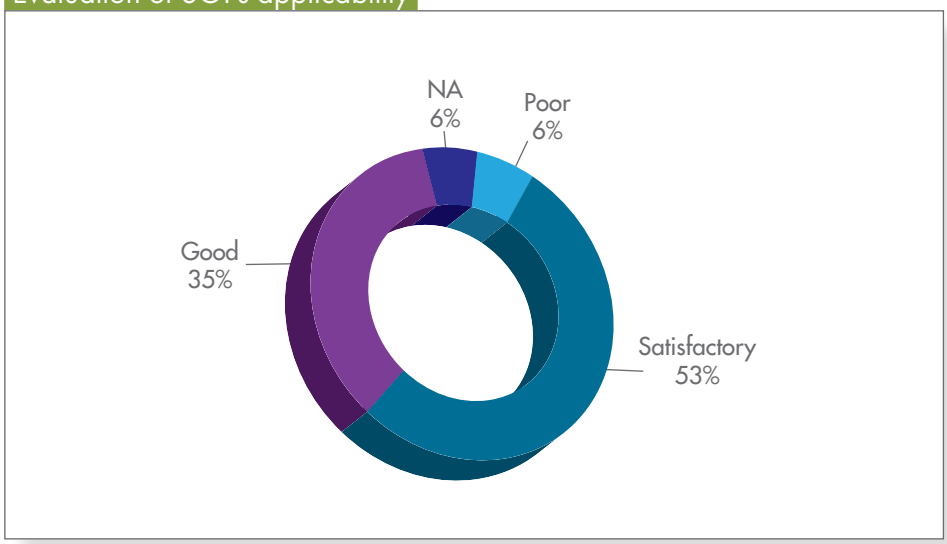
For participants, **SOPs were clear, workable and a good basis** for collaboration. *

Evaluation of the clarity of the SOPs



*

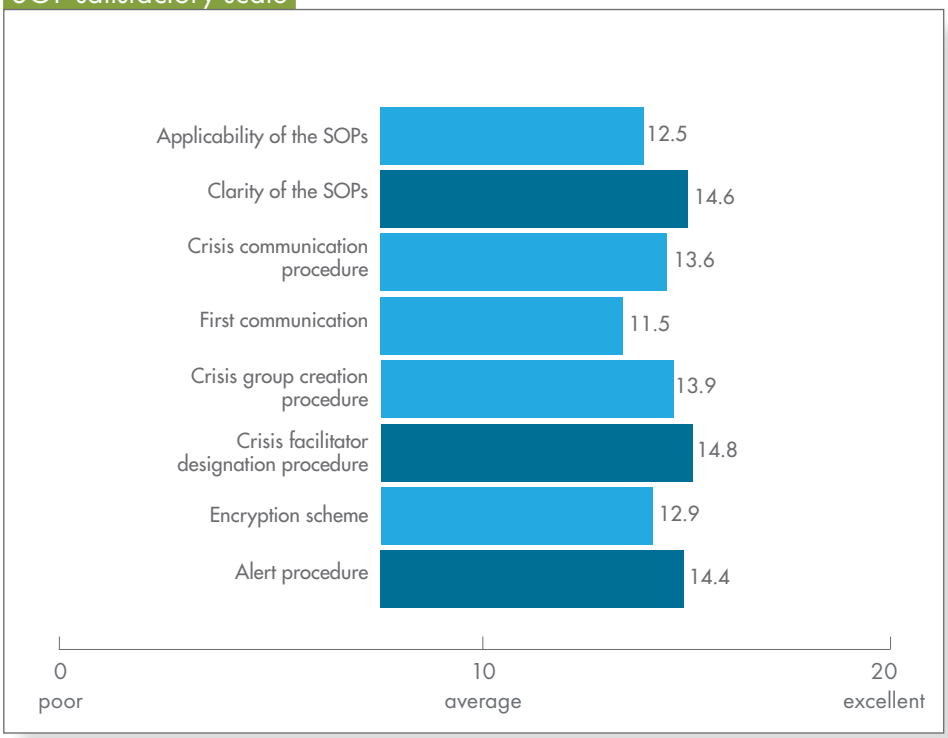
Evaluation of SOPs applicability



*Some paragraphs have intentionally been removed for confidentiality reasons.

3.4 Recommendations on SOPs

SOP satisfactory scale



3.4.1 Alert procedure

*

3.4.2 Encryption scheme

*

3.4.3 Crisis facilitator designation procedure

*

3.4.4 Crisis Group creation procedure

*

3.4.5 Crisis communication procedure

*

3.4.6 Clarity, applicability and general comments on SOPs

*

*Some paragraphs have intentionally been removed for confidentiality reasons.

3.5 Recommendations on Media Training

Lessons learned and recommendations following this media training could be summarized as follows:

✓ To **assess the importance/impact** of a newspaper or a TV channel calling for an interview.

✓ When first requests for interviews are made, cyber defence agencies might not have yet established their communication strategy. Considering that no pre-defined answers are ready, Public Relations officers should:

- **Take notes** and suggest that the journalists to call back later.
- **Spread the message** across the agency, ministries and counterparts to define aprecise communication strategy.
- **Provide journalists with the PR contact** of the administration responsible for handling the media if the agency is not authorized to communicate on the crisis.
- **Provide general information** about the agency and use interviews as an opportunity to reassure their interlocutors in case the agency is not able nor authorised to answer technical questions ("the team is currently working on it", "resources are mobilized", "active collaboration between services and MS",...).

✓ **To set up a schedule for the media** as early as possible to take pressure off and to better control the timing of communication. (Indicate if a press release will be sent, by whom, at what time? Will the agency organise exclusive interviews/press conference? When?).

✓ **To coordinate the timing** with other stakeholders or counterparts.

✓ In order to appear as a transparent organisation, PR should **provide information on communication policies.**

CEIS
280 Boulevard Saint Germain
75007 Paris
ceis@ceis.eu

CEIS - European Office
Boulevard Charlemagne, 42
1000 Brussels
bruxelles@ceis.eu

Some sentences or paragraphs have intentionally been masked or removed for confidentiality reasons. A full version of this report has been realized and printed for Public Authorities involved. The aim is to avoid any leak about security measures and procedures.

If you think that you could be a relevant receipt for the full report, please contact : bruxelles@ceis.eu
The request will be assessed with the partners of the consortium.