MULTILATERAL MECHANISMS
FOR
CYBER CRISIS COOPERATION

2nd international conference on cyber crises
23 September 2013, Athens, Greece
Adrien Ogee, ANSSI

As of 2009, “cybersecurity” was still a buzzword in the EU.

If the 2009 Critical Information Infrastructure Protection Conference in Tallinn paved the way forward, at the time, European cooperation in the field of cybersecurity was stammering at best.

Over the last 4 years, Member States have allocated budgets, time and resources to European cooperation in cybersecurity and EU institutions have been at the origin of numerous initiatives.

The growing size and visibility of the impacts of cybersecurity crisis is striking. The capabilities for mass disruption exist for many years. There are each day more groups with intent to disrupt our critical services. It is just a matter of time between those two combine.

The present security level in Europe is not satisfying but we need to recognize the pace with which we are all trying to catch up. Countries are now aware of the potential multinational scale of cybersecurity crises, and the absolute necessity to cooperate internationally to mitigate these.

Just a note: in this presentation, I call a cybersecurity crisis or cyber crisis an event or a series of events, natural or man-made, qualified as a cyber-crisis by a MS. A *multinational cyber crisis* is defined as a cyber crisis which causes or impacts concern at least two MS.

Generally, exercises are designed to test existing procedures or organizations.

As of 2010, in the EU, there was no procedure, no directory, nothing to drive cooperation during a cyber crisis between EU Member States, apart from traditional non-crisis CERT channels and non-cyber political-level crisis agreements.

Cyber Europe 2010 was a top-down initiative. Clearly, participants did not feel the need to exercise. They were wrong.

The exercise served as an electroshock.

The truth is the exercise was chaotic (which is positive!).

MS exchanged information in an uncoordinated fashion.

Participants crawled under emails and phone calls.

Information overload prevented crisis exits to be even considered.

There was no operational picture and little crisis governance.

The main lessons of Cyber Europe 2010 were that CERTs communities are well equipped and prepared for national and sometimes even multinational incident handling, but certainly not for large-scale crisis management. Large scale crises require a lot more than information exchange.

Because their impacts are not confined to information security circles anymore, such crises require the capability to take into account non-technical information (public affairs dimensions, political agendas, diplomatic relations…) and the ability to convey the right messages to the political actors.

International crises require international cooperation and for fast mitigation, you need common agreed, predefined and exercised processes. You need staff that is not only prepared to work in an international environment, you need staff that is willing to do so despite natural reluctance due to the issues at stake.

Given that:

-sharing is the basis of cooperation

-Cybersecurity is often sensitive and sovereign

-Information & capabilities lie in the member states

We assessed that for European crisis cooperation activities to be efficient, it had to be a shared responsibility between all Member States. Indeed, we assumed that only by feeling concerned, invested of a role, and by participating to development of the associated plans and procedures, would EU member states slowly improve their international crisis management capabilities.

Therefore, we felt the need to own, *rather than externalize,* crisis management planning.

To do so, we agreed to pursue first a bottom-up approach by involving directly all EU cybersecurity crisis managers. The idea was to build around their knowledge while involving them in the creation of new plans and procedures, which was a way to build trust and to ensure that they would all know, use and promote, the mechanisms that were being developed.

This has been the most important driver of our work these last four years and I believe that all of us who worked on these mechanisms would say that it was the right

approach.

In order to put theory into practice, we came up with the a plan that looked like this:

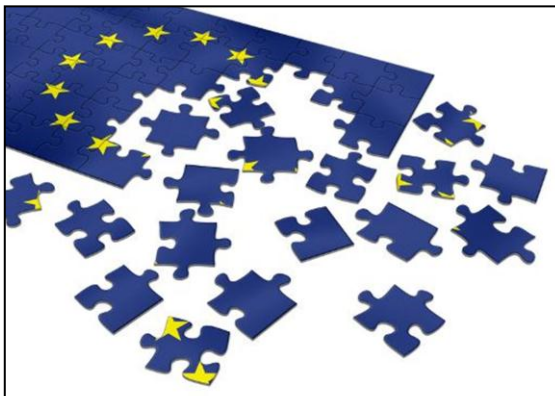
MAP all the relevant stakeholders: create a directory, first step we conducted

DEFINE the relevant crisis management levels: the European Cyber Crisis Cooperation Framework, to be presented right after, is a framework which defines all the different crisis management levels

CREATE cooperation procedures: the European Standard Operating Procedures

EXERCISE and improve: define an exercise roadmap

I have to be honest with you: this plan was not as crystal clear when we started working. It seems as we had this nice approach right from the start but we did not. You have to consider that we are 27 European countries, plus 4 other countries from the European Free Trade Association, that participated fully in all this work. Agreeing, just agreeing on something, was already a big victory. So it took us much time and effort just to convince each other to pursue one or another direction but I guess it was very positive in the sense that we always ended up with a real good, solid and backed-up plan !



[ECCCF]

THE EUROPEAN CYBER CRISIS COOPERATION FRAMEWORK

7

The first step towards cooperating is knowing each other, what to expect and building trust.

EU MS cybersecurity organizations are numerous and have different and sometimes overlapping mandates.

Although a directory was quickly and relatively easily compiled, it did not reflect the heterogeneity of the mandates of all stakeholders.

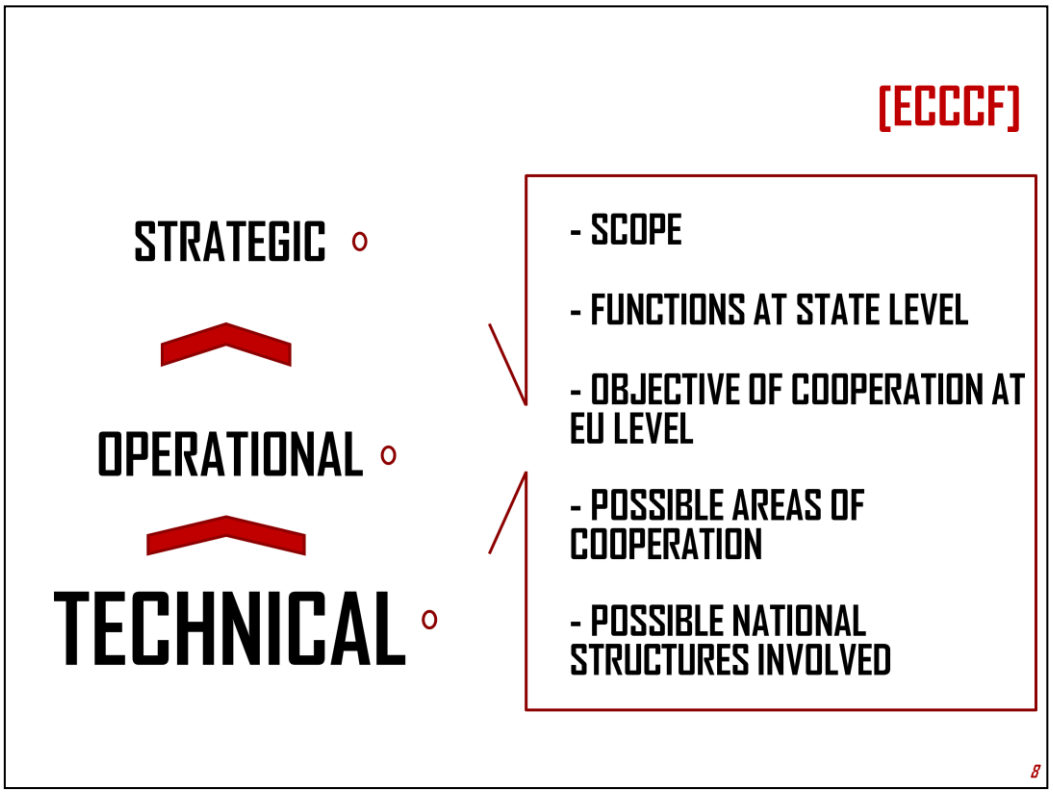
Therefore, it became obvious that to effectively work together we had to agree upon generic crisis management functions to determine what can be expected from each entity that has a responsibility in cybersecurity in each EU MS.

It was also necessary to map existing crisis cooperation procedures to identify the missing bricks.

What it is

Developed in 2011-2012 by a handful of EU MS, the ECCCF is a triple-layered non-binding cybersecurity crisis cooperation framework for public organisations.

It defines generic crisis management functions for each of three layers which are: technical, operational and strategic.



For instance at the Technical layer you would find

- *Scope*: Incident handling during a cyber crisis
- *Possible national structures involved:* CERTs

At the Operational layer one would find

- *Scope*: Management of the technical causes of the cyber crisis
- *Possible areas of cooperation*: threat analysis, risk assessment, technical mitigation measures, etc.
- *Possible national structures involved*: cyber defence/security agencies, CERTs, IT ministry, regulators, communications authority, etc.

Last, at the Strategic layer

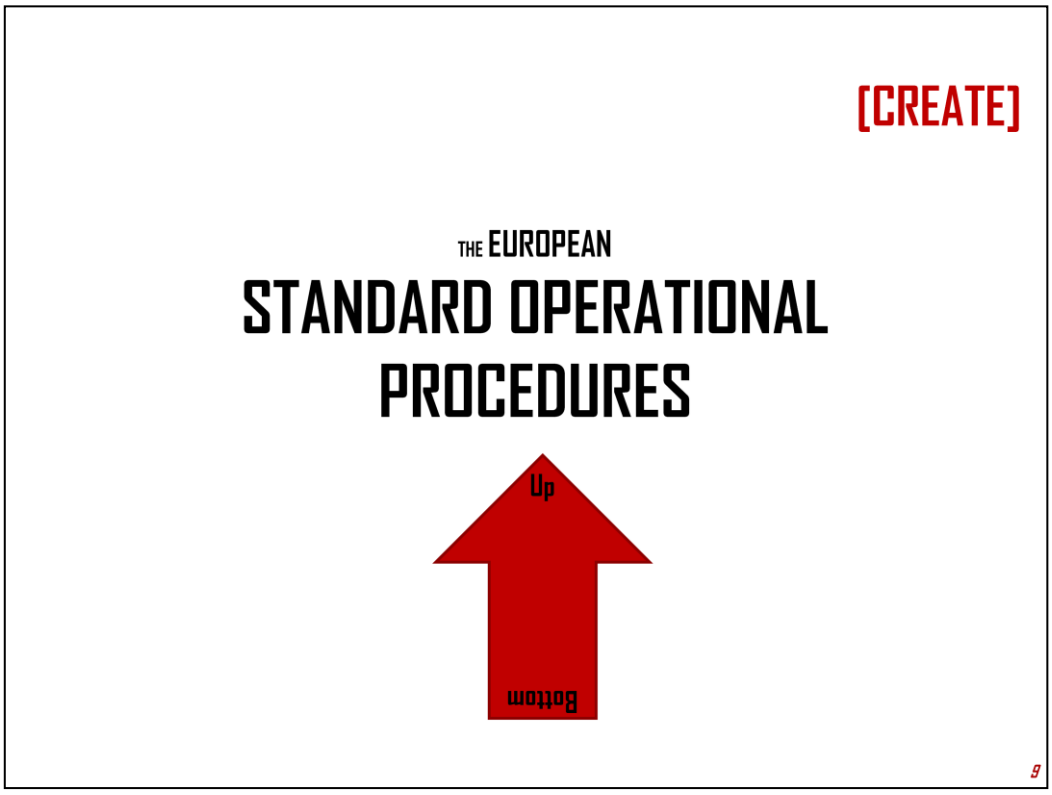
- *Scope*: management of cyber and non-cyber aspects of the crisis
- *Possible areas of cooperation*: crisis communication (between MS and EU), high-level decisions including cross-border aspects of the crisis, civil protection, etc.

The ECCCF also describe what we call building block, that is the existing crisis cooperation procedures available for each of these levels.

At the technical layer, although there is room for improvement, it has been assessed that CERTs had long-standing communication exchange procedures or at least understandings that worked sufficiently well for them to know how to pass on information to one another.

At the operational level though, there was nothing. This was the next item on our plan, which I already touched upon earlier, and which I will describe further on the next slides.

At the strategic level, we identified that there were already existing European crisis management procedures, namely the crisis coordination agreements. Although these did not cover explicitly cyber, it seemed like a good enough basis and until now, I admit that it was a little out of our focus, mainly because we were willing to work bottom-up and in that sense, close the work at the operational layer before engaging the strategic slash political level. Nevertheless, it is the next item on our agenda and next year, Cyber Europe 2014 will already allow us to test the crisis coordination agreements and see how we can improve them, if necessary at all.



What it is

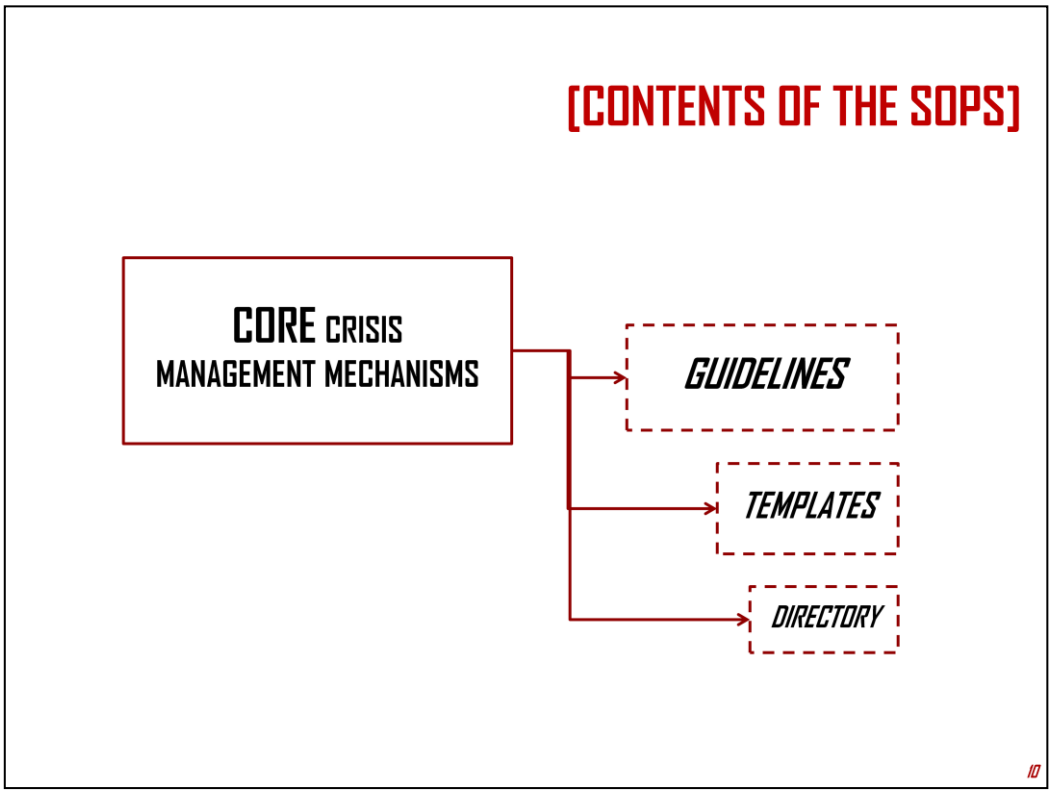
The SOPs were launched in 2011 with a pilot programme composed of a handful of MS.

It was, and still is, a bottom-up practical procedure written by and for EU cybersecurity crisis managers.

The SOPs address the operational level only. They structure crisis management activities so that an operational picture can be drawn upon the technical information shared on an international basis and presented to the strategic (/political) level for decision making.

Objective:

"To provide a set of good practices to improve information exchange and cooperation at operational level between countries during multinational cyber crises, in order to fasten the understanding of their causes and the mitigation of their impacts".



The SOPs is a 40 page document which contains information about the following:

The first chapter Core crisis management mechanisms describes the key principles to European operational crisis management. Without going into too many details, the heart of the SOPs lie in the creation of a crisis group, which is led by a crisis facilitator, being one or more Member States impacted by the crisis. All members of the crisis groups then engage into crisis cooperation activities, which tempo is defined by the facilitator. They exchange situation reports at certain times, participate to chats, audioconference or VTC depending on capabilities and needs, and try to come up with a plan, as a group, as fast as possible. The concept we developed tries to focus on speeding up the mitigation of the impacts, by understanding faster the causes.

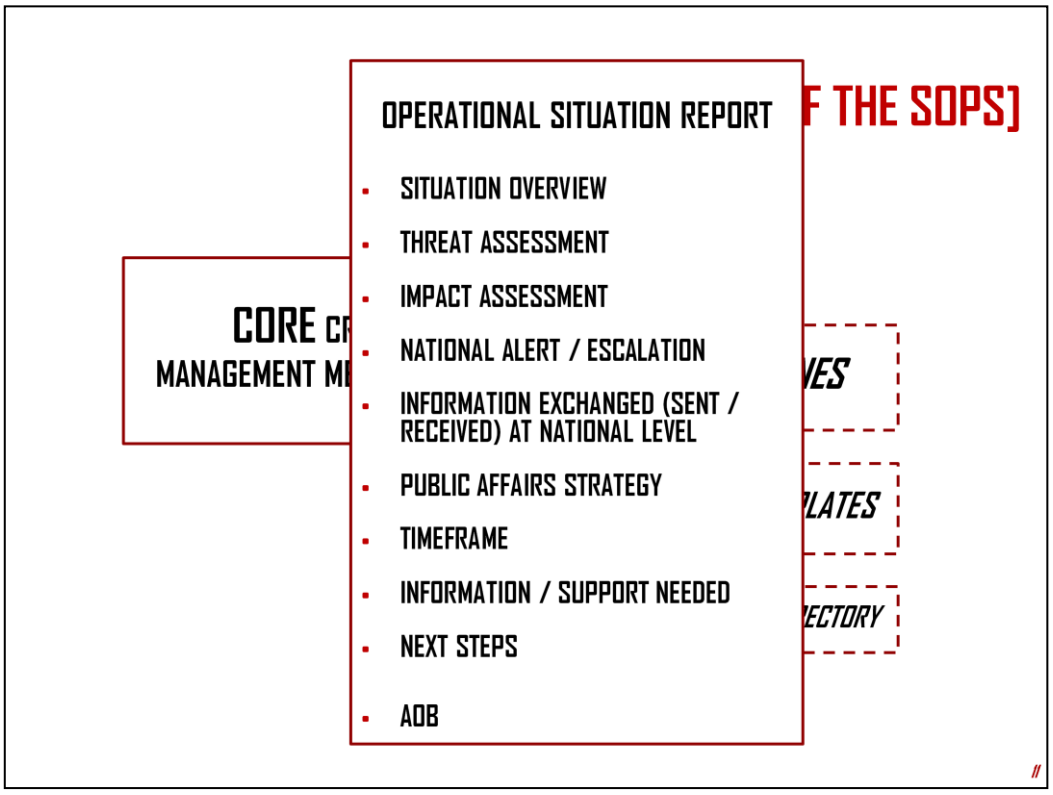
There is a lot of common sense in the document, it is not reinventing the wheel, just trying to make classical crisis management principles fit to cybersecurity needs.

In order for the SOPs to be as practical as possible, that is, as usable as possible in times of crises, we decided very early on to have guidelines so that newcomers would understand very quickly the group dynamics and what would be expected from them. There are over a dozen of these guidelines and they provide great tips on several topics, from sending an alert, to being a crisis facilitator, adopting a crisis-group structure depending on criterions such as threat, impacts, number of member

states involved etc., to the type of information that should be shared and ways in which non-EU members, public or private, can participate.

Finally, to speed things up ever more, we created some generic templates for information exchange, for instance a generic situation report, an APT-specific situation report, a typical agenda for crisis meetings, etc.

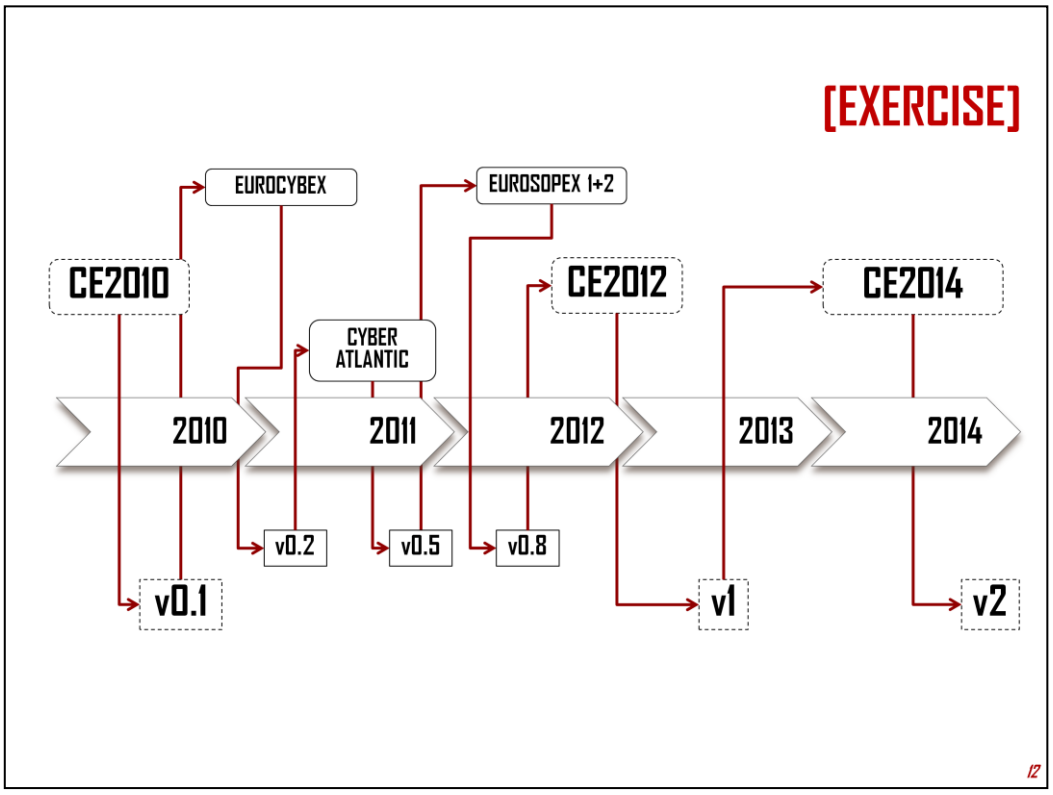
Lastly, the SOPs contain today the directory that we created right after Cyber Europe 2010, so that EU crisis managers have everything they need in the same document.



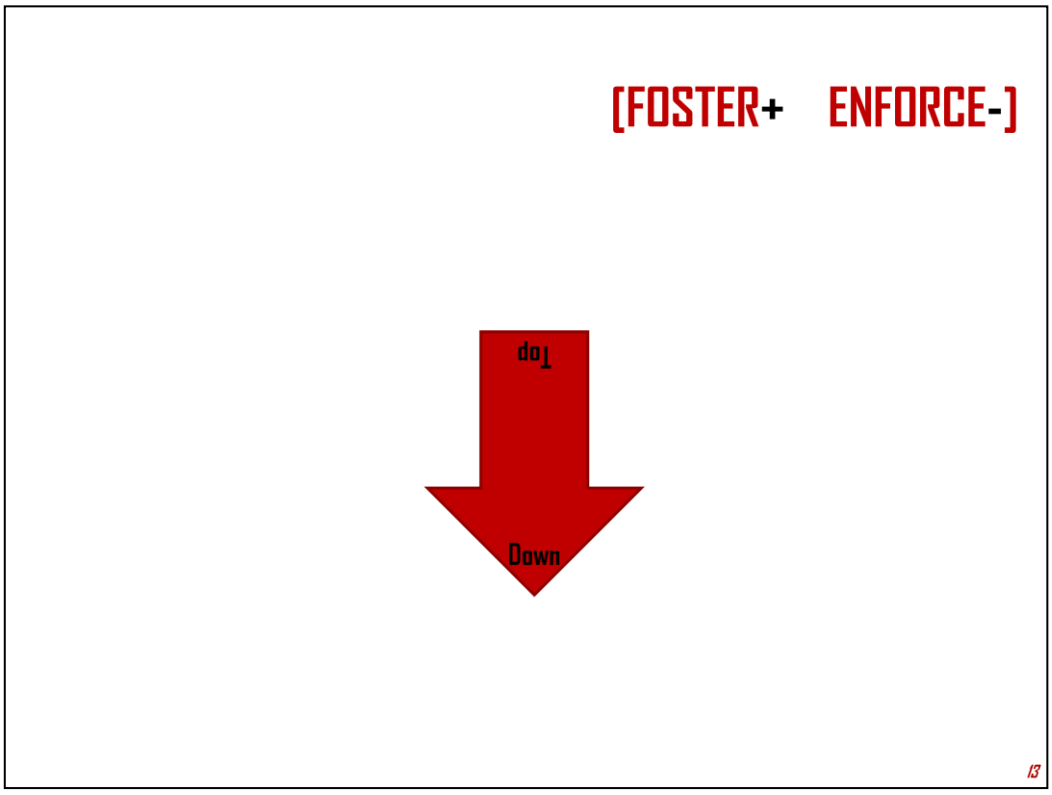
Here you can see the generic operational situation report.

These categories are the info that we want EU cybersecurity crisis managers to be able to exchange. You see that it requires more than just compiling lists of IPs or SNORT rules, even though at the end of the day, these reports will end up containing a lot of very technical information.

OK, I don’t want to spend much time on this, it was just an example for you to see what level of information we seek to exchange.



I really wanted to show you this slide because it reflects the truly bottom-up development of the SOPs. After Cyber Europe 2010, which was a top-down initiative (and this was good, we needed it), we decided, us, European member states, that we needed to participate fully in the creation of the cybersecurity sector in Europe. We decided to create this exercise plan, which you cannot see here but is incremental (meaning that every time we exercised, we did either something new, either something additional to the previous iteration). This way, we were able to have the SOPs go through 6 different multinational exercises in less than 2 years, and a lot more rounds of comments (I counted 25).



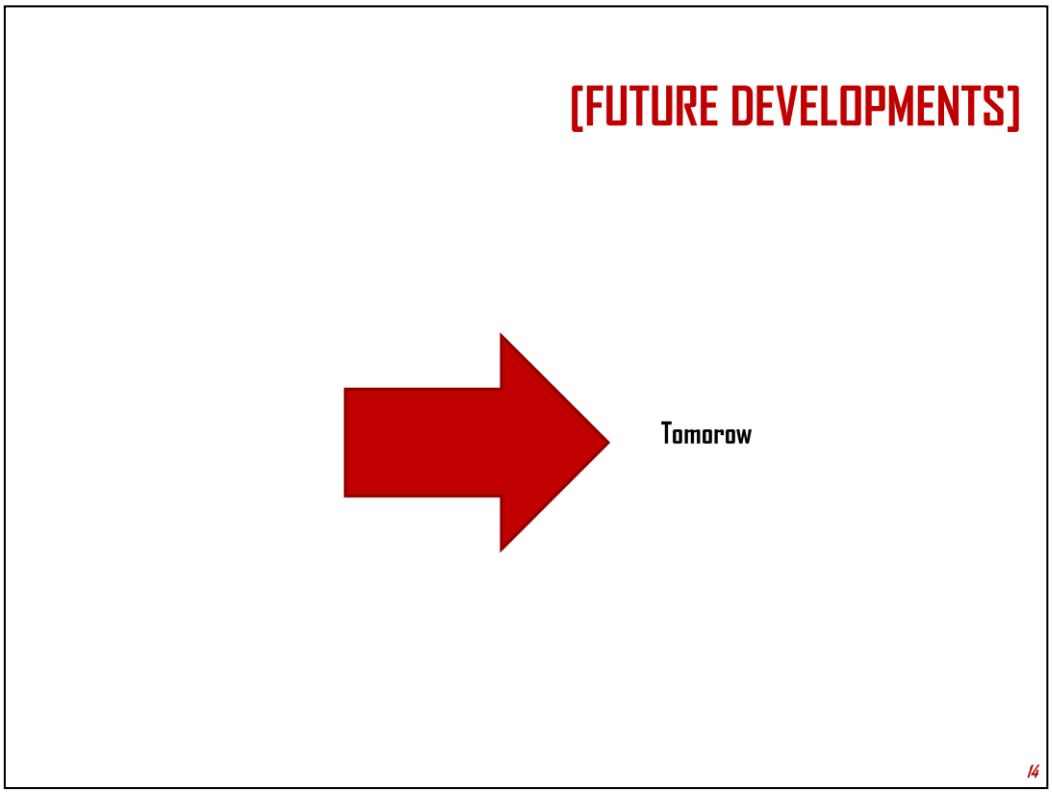
Many initiatives have been undertaken by the EU Commission, in an effort to contribute to the improvement of cybersecurity capabilities and cooperation.

To name but two: the Cyber Security strategy and the draft NIS directive (both released early 2013)

Although these are top-down initiatives, they build upon some of the key findings of the bottom-up work that has been going on since 2010. The directive also introduces obligations, which are being discussed by the Member States right now.

One key lesson learnt from the work I have been involved in these past 4 years, is that for cooperation activities to be successful, all stakeholders need to feel invested. Recognising the sovereignty of some (not all) cybersecurity issues, we feel that the Commission, as it has been the case these past four years, should be more on fostering than enforcing. I am French and I can tell you that our legal code is pretty big: my experience tells me that results only come with good balance between cooperation based development and top-down enforcement.

The ENISA has been a true partner in all these years and has greatly contributed to improving EU cybersecurity defences. I invite all EU policy makers to invest and rely more on its people.



1/ Release and publication

I like to think of the EU SOPs as the common DNA of EU cybersecurity crisis managers. Right this moment, the document is being typo-checked and translated in all EU languages. It will be officially released for European Member States before the end of the year. Also, the document will be shared with all relevant stakeholders, outside the EU.

2/ Cyber Europe 2014

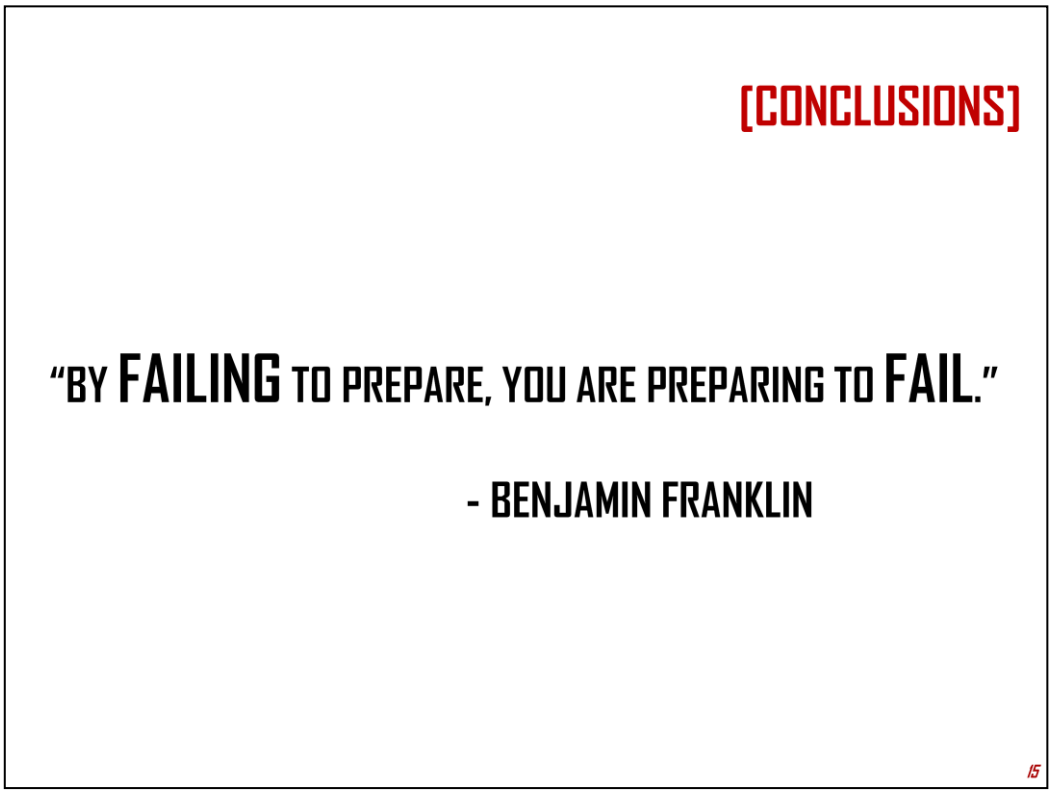
The next item on our agenda, as I mentioned earlier, is to foster cooperation at the political level, while continuing the development of technical and operational level procedures. To meet this end, Cyber Europe 2014 will be a triple-layered exercise: technical, operational, political. Although the details are still under discussion, we are most probably going to have not one but three exercise, to make sure that each level gets the attention it needs. We did not feel ready yet to have a full-fledge exercise with all levels involved. Maybe next time.

During Cyber Europe 2014, we hope that based on the technical information compiled in the technical exercise, a common operational picture will be created using the SOPs in the operational exercise, and provided to the leadership during the strategic exercise.

3/ Re-using the SOPs

The last item on my mind, and this is something that I wanted to do for a long time already in France but couldn't find the resources yet, is to promote the SOPs to other circles and notably, to the private sector. The SOPs can easily be adapted to other contexts, to serve other organizations or sector. The banks have not waited for governments to learn how to work together, but I am sure they might see added value in reading the SOPs and developing their own if they have not. Other sectors are not that advanced and could catch up a lot faster in terms of cooperation with their peers if they were to benefit from our experience.

The details of when and how we can share all this still need to be worked up –we wanted to have a version 1 first, but to any community that would benefit from such multilateral cooperation, mechanism I would recommend following a path similar to ours, with a discovery exercise first, and the drafting of a plan and procedures next. I guess it is a good thing Cyber Europe 2014 will involve the private sector, right ?



Thinking that it is only by developing your own capabilities and systems that you will ensure the cybersecurity of your network, of your company or your country, is deeply wrong. Cybersecurity is a global issue and cybersecurity crisis mitigation also.

In the EU, we have chosen the path of shared responsibility. This is not the only option. Central governance has other virtues, that just seemed not applicable to our political configuration at the time but that could perfectly work for you. In all cases, you need all the stakeholders of your crisis management framework to feel invested and to be trained regularly. Independently from the path you choose to take, the only way to achieve this is the one of thoughtful governance: the perfect balance between bottom-up and top-down initiatives.

While developing your multilateral cooperation frameworks, mechanisms and exercises, do not underestimate, sensitivity, sovereignty and the cyber fog of war that will increase the complexity of cooperation in the field of cybersecurity to a point that the existence of cooperation frameworks and mechanisms do not ensure positive crisis outcomes.

Nevertheless, the lack of such frameworks, mechanisms, and the lack of professionalism of your staff (notably if they don't exercise), is the only way to ensure they will systematically fail at crisis cooperation. This is what I wanted to illustrate with this quote from Benjamin Franklin.

I hope that you enjoyed my presentation. Thank you for your attention.