Minutes of the Meeting of the NLO Network of 30th January 2018

Meeting:	ENISA NLO Meeting – 30th January 2018
Location:	ENISA Athens premises
Date:	12/03/2018
Attendees:	Katharina Boitner (AT), Phédra Clouner (BE), Roman Packa (CZ), Flemming Faber (DK), Gert Auvaart (EE), Eirini Athanasiou (EL), Heidi Kivekäs (FI), Samuel Rothenpieler (DE), Anita Tikos (HU), Thorleifur Jonasson (IS), Davide Nardacci (IT), Vaidotas Ramonas (LT), Laurent Weber (LU), Matthew Yeomans (MT), Hans Oude Alink (NL), Gunn Pettersen (NO), Robin Bakke (NO), Magdalena Wzosek (PL), Isabel Baptista (PT), Rastislav Machel (SK), Peter Wallström (SE), Heather Butler (UK) **ENISA:** Steve Purser (Chair), Paulo Empadinhas, Evangelos Ouzounis, Aidan Ryan, Paraskevi Kasse, Anna Sarri, Prokopios Drogkaris, Marnix Dekker, Katerina Christaki, Florian Pennings, Olivier van Geel
Apologies:	BG, CY, ES, FR, HR, IE, LV RO, SI

Introduction by the Chair

The Chair, Mr. Steve Purser, welcomed the NLO Network to Athens, and opened the agenda with sharing relevant information and background on the EU cybersecurity package, published last September. Mr Purser continued to demonstrate the relevance, importance and necessity of this package (including the mandate proposal of ENISA) for the EU and its MS.

Concerning the mandate proposal, certification and Blueprint are two new elements for ENISA. Mr. Purser clarified ENISA's position to the NLOs on:

- Certification: ENISA will not be 'doing certification' unilaterally. ENISA will work together with the communities that need to be involved.
- Blueprint: The Blueprint is not defined as a solution for all issues, but it provides an instrument to utilize and optimize European cooperation. Lastly, ENISA has no ambition of becoming a 'CERT'.

The proposal on EU Certification seems to be inspired by (EU) 765/2008 that provided the CE mark fundament. The objective of the proposal is to establish an EU valid and supported certification model. The EU needs to address market fragmentation, and by doing so look at best practices. For example, SOG-IS is experienced and can serve as starting point. Nevertheless, there are many challenges, such as the reach and scope of the proposal (very wide, it covers many devices). Mr. Drogkaris further addressed this topic in the meeting.

Update on the activities of the NLO network and adopted guidelines of operation

On behalf of ENISA, Ms. Katerina Christaki, NLO network coordinator and PoC at ENISA, warmly welcomed the new NLOs from Estonia, Poland, and PoC at the European Commission.

Looking forward to 2018, ENISA organized the first meeting in January and took this opportunity to address and invite the NLOs for a discussion on the *Guidelines on missions, principles, and functioning of the NLO network* that were adopted by the MB in 2017. According to these guidelines the NLOs should proactively share information on NIS developments in their MS, but ENISA should also give the NLO network priority in contacting the public and private sector in Member States; ENISA and NLOs should meet twice a year, instead of once and one of these meetings, at least, should be a physical one.

With the newly adopted guidelines in mind, Ms. Christaki kindly invited the NLOs to further discuss at the meeting the enhanced role of the NLOs, the (new) working methods and tools, and finally in the afternoon session, the MS input to WP2018.

Action: All NLOs to (more) proactively share with ENISA PoC information on relevant NIS developments in their MS, such as relevant events, policy developments, industry cooperation/PPPs, etc.

Action: NLOs provide input to ENISA PoC in advance of the second NLO meeting of 2018 in preparation of a report to be presented at the Ordinary Meeting of the Management Board as per the adopted 2017 Guidelines.

Tour de table, NLOs

The NLOs provided their views on: involvement at ENISA activities and/or groups in 2017; on ENISA requests to the network; and on challenges/opportunities.

Involvement in ENISA activities:

It becomes clear that many NLOs have been involved in at least the following program activities of ENISA: the European Cyber Security Month (ECSM), European cybersecurity exercises, and the European Cyber Security Challenge (ECSC). Besides that, some NLOs are involved in, or actively informed about the NIS Cooperation Group and the CSIRTs Network. Thirdly, a large part of the NLO Network is active in one of the expert groups, or in the Art 13/19 working groups that are coordinated by ENISA. Parallel to this, it becomes clear that on the side of ENISA these NLO activities have remained unknown until now. The NLOs are therefore kindly requested to actively inform ENISA PoC for the NLOs on their participation with ENISA, and ENISA's PoC for the NLOs will liaise (more active) with the responsible ENISA project managers.

Challenges:

- One of the main challenges of the NLOs is their (limited) capacity in terms of how much time can be spent on the NLO Network in relation to the work for your own organization. Logically, in most cases priority is given to work that directly connects to one's organization.
- Another challenge is 'being informed' and kept informed by either ENISA or the colleagues of the NLOs. In some cases it turns out that cooperation already exists and is considered valuable, but that there was no communication about it.
- The relationship among the ENISA Management Board, the NIS Cooperation Group, the CSIRTs Network, and all the (sub) working groups involved, make it difficult for the NLOs to not only keep a clear view on all (relevant) activities but also on relevant decision making and strategy building. There is a call for a clearer view on the differentiation and overlap of all the collaboration groups.

Opportunities:

- The fact that the NLO meeting is organized in the beginning of this year, is an opportunity to better align the NLO activities to the ENISA Work Programme, studies and events from early on. This allows the NLOs to have a better overview of what is needed and plan ahead;
- Use the mandate discussion to further clarify or even formalize (following Polish proposal, addressed later on the day) the role of the NLO network;
- The NLOs can be the 'translators' of what the Management Board has defined in the Work Programme of ENISA.

During the tour de table the following requests are defined:

- Request from the NLO Network to ENISA to provide more structured information on all its activities such as projects and expert groups (Will be addressed as last point of the agenda);
- Request from ENISA to the NLO Network to familiarise themselves with the recently adopted *Guidelines on missions, principles, and functioning of the NLO network* and provide input on the Guidelines;
- Request from ENISA to NLO Network to actively share previous, or planned involvement in ECSM and ECSC.

Update on the implementation of the NIS Directive

Ms. Paraskevi Kasse (ENISA) provided the NLO Network with an update and overview of the NISD implementation activities after its adoption in 2016. ENISA informed the NLOs on the Agency's role concerning the NISD (implementation), the challenges achieved and successes thus far. More in depth, ENISA informed the NLOs on the several working streams that have been executed on the request of the NIS Cooperation Group. ENISA informed the NLOs that one issue is that there are limited resources. Another kind request from ENISA to the MS, via the NLO Network, is to delegate the right experts that understand the technical challenges, specifically concerning the Operators of Essential Services (OES).

The EU Cyber Security Act: Certification

Mr. Prokopios Drogkaris (ENISA) gave a presentation on ENISA's activities in ICT cybersecurity certification, with a view to the Commission's proposal for a Cybersecurity Act. He noted that this year, ENISA would focus on existing national initiatives and how these could be mapped onto EU cybersecurity certification schemes.

Some clarification was provided on the functioning of the proposed EU cybersecurity certification framework encapsulated in the proposed Cybersecurity Act. It was underlined that, according to the Commission's proposal, ENISA could not initiate the process for adopting a scheme by itself. This role would be taken up by the Commission, or the European Cybersecurity Certification Group, where the Member States are represented by their National Certification Supervisory Authorities. Furthermore, it was noted that Member States would be involved through other avenues including, for example, the adoption of implementing acts.

It was further emphasised that ENISA is not assigned the role of a certification authority. ENISA's role is to liaise with the ECCG and other stakeholders to reach a consensus in the preparation phase. It was also noted that national schemes and European schemes could co-exist, provided there is no overlap.

The Chair then opened the floor for questions. A question was raised on the specific method for addressing the area of certification within the organisation, and the possible role for the NLO Network. The Chair noted that the new mandate proposal involves (roughly) a doubling of the ENISA budget, and includes a

rough mapping for the new resources. It was noted that, in this new area, ENISA would work by bringing together experts from the Member States and Industry for detailed discussion, where a role for the NLO could be foreseen.

Update on the National Cybersecurity Strategies – activities

Ms. Anna Sarri (ENISA) gave a presentation on ENISA's work on National Cybersecurity Strategies (NCSS). She noted that all 28 MS have adopted a NCSS and some have already updated these strategies into new versions. ENISA supports MS with the ENISA NCSS map, reports, the expert group and art. 14 requests. A yearly workshop has been organised since 2013, the next of which will potentially take place in Helsinki, Finland (under discussion). It was explained that key activities in 2018 include a tool to evaluate NCSS, an update of the map, and a toolkit to create national ISACs. MS may support ENISA by, for example, providing PoCs for the NCSS expert group.

It was noted that LU concluded its 3rd NCSS, which is expected to be applicable from March 2018. It was agreed that, in relation to the request for input on the proposed evaluation tool for NCSS, ENISA would circulate a list of options to the MS.

New Awareness Raising Portal on MS Activities

Mr. Paulo Empadinhas (ENISA) gave a presentation and opened the floor for feedback on the proposal, discussed at management board level, to create an awareness-raising portal on MS activities. He noted that EU citizens and businesses often do not know where to find information, and that a portal could present one option to overcome this challenge. In this regard, ENISA would like to assess the opinion of the NLO Network on how feasible and interesting it could be to create a portal aggregating MS information and best practices.

The case of exchange between BE and FR was cited as a success story. However, it was noted that similar efforts had been discussed before and abandoned due to problems such as the language barrier and that duplication with other efforts in the framework of the European Cyber Security Month would have to be avoided.

Other MS noted that such a portal could focus on the description of campaigns and awareness raising efforts as well as the impact these campaigns had, rather than just sharing material in a language that should be translated. Providing all information in English could also help in altering the language barrier, previously encountered in similar past efforts.

Action: ENISA will share a proposal to the group in Q2 2018, and the NLO Network will indicate whether it wants to move forward or not.

Polish Proposition about NLO and Update from Poland

In the framework of the ongoing legislative process for the Cybersecurity Act, PL has tabled a proposal to include the NLO network in the Regulation (i.e. formalise the NLO network) in Art. 12(a). PL holds that this would help establish a clearer role for the NLO network. So far, four other MS support the proposal (FR/HU/FI/EE). PL states that the proposal is basically in line with the MB Guidelines adopted in 2017, but creates a formal legal basis for the NLO network in the Regulation, involving a minimum of two meetings and at least one physical meeting per year.

In relation to the proposed legal text and the avoidance of duplication of efforts, the Chair enquired as to how this can be realised considering the existence of various other relevant working groups related to the ENISA Work Programme. Some MS replied that officially involving the NLO network would help clarify its role. In relation to defining a role for the NLO network, it was noted that, where the MB makes big

decisions, the NLO network is more involved in the implementation of these decisions (i.e. the "how", while the "what" is decided by the MB). WP alignment was identified as a challenge that could be associated with this approach. It was also noted that smaller MS may have problems to obtain the necessary resources for an obligatory role. It was further noted that a formal legal basis could facilitate ENISA's work with the private sector. PPPs were identified as a potential area of interest for the NLO Network.

Secure by Default – UK policy review

Since early 2017, the UK has been conducting a policy review focusing on identifying measures to improve security by design in IoT products. The review, which was done in collaboration with industry (expert advisory group), is final and will be published in the weeks following the NLO meeting. The key output of the review is a code of practice.

Other proposals to be discussed in the UK in 2018 that were mentioned are 1) voluntary labelling schemes; 2) training and professional bodies; and 3) regulatory options.

In the discussion, the question of how information sharing can be applied effectively within the NLO network was addressed. It was noted that, taking the example of ENISA's Permanent Stakeholders' Group (PSG), the network could consider the value of incorporating Working Groups in its *modus operandi.*

CCB and Cert.be

An update was provided on the Belgian CCB and Cert.be. The Belgian NLO described the organisational structure of cybersecurity in BE, and the strategic objectives of CCB, as well as its role as an enabler. Some key projects, including the Early Warning System to exchange information about vulnerabilities, were mentioned. In relation to Cert.be, it was noted that a staff increase is foreseen for the period of 2018-2019 to facilitate 24/7 capabilities.

Resources and staff exchanges between MS were brought up in the discussion, though it was acknowledged that such exchanges could be more challenging for organisations with fewer human resources. It was noted that it would be good to have an overview of the kind of expertise available, and how to make use of it.

The aspect of PPPs was also discussed, and it was noted that ENISA has done quite a lot of work on this, and can support MS where necessary. A question was raised regarding the BE cyber diplomacy framework which, as was explained, constitutes a mechanism to follow international affairs around cybersecurity. It was also clarified that the BE ICMS/Cobra tool is used to exchange information in incidents. The Commission's MeliCERTes facility, which is designed for information exchange between governmental CERTs, was mentioned as a possible tool for the NLO network to look into.

Transposing the NIS Directive in Slovakia

An update was provided on the transposition of the NISD in SK. It was noted that the transposition process began in mid-2016, roughly 3 months after adoption, and that the NIS implementation act is in its final stages, with expected adoption on 1st March 2018.

One aspect that was discussed was the distinction between physical security and cybersecurity, where the potential physical impact of cyber threats should be kept in mind by governments. It was noted by ENISA that the scope in certain fora is getting blurred and fragmentation was identified as an issue to be watched. In this regard, it was mentioned that various actors and departments are often involved, and that sectorial work on cybersecurity is increasing.

Discussion on MS contribution to the WP2018

The Chair, with support from Mr. Evangelos Ouzounis (ENISA) and Mr. Prokopios Drogkaris (ENISA), gave a presentation on the ENISA outputs, expert groups and procurement for 2018. The objective was for the NLOs to get an understanding of ENISA activities and how to contribute.

The expert groups mentioned were the following:

1) The IoT Security Expert Group (IoTSEC)
2) ENISA ICS Stakeholders Group (EICS)
3) European SCADA and Control System Information Exchange (EuroSCSIE)
4) ENISA Threat Landscape Working Group
5) Article 13a Experts Group
6) Article 19 Experts Group
7) eHealth Security Experts Group
8) Expert Group on Finance (EGFI)
9) Cars and Roads Security (CarSEC) Expert Group
10) Internet Infrastructure Security and Resilience Reference Group (INFRASEC)
11) Transport Resilience and Security Expert Group (TRANSSEC)
12) Cloud Security and Resilience Experts Group
13) National Cyber Security Strategies Experts Group
14) European Cyber Security Challenge
15) European Cyber Security Month
16) Cyber Europe Exercise

ENISA informed the NLOs on the various existing expert groups. Applications from MS to the groups that they are interested in are welcome. It was also noted that, where some groups are more active than others, the tendency at ENISA is to keep expert groups alive in order not to break communities that are challenging to build. NLOs were invited to contact ENISA should they feel insufficiently involved in expert groups.

In relation to how expert groups are involved in the work of ENISA, it was noted that ENISA takes full responsibility for publications, where expert groups may be used (for example) for interviews, input, and workshops. The set-up of these groups is generally flexible and the kind of involvement may vary per group, e.g. public sector more involved in CIIP, industry where it concerns IoT. The groups are involved as part of the evaluation procedure, where peer review is considered an important step.

It was also noted that new expert groups may be organised in 2018. Furthermore, there was a call for participation of the NLO network in ENISA's work on Industry 4.0. It was noted that ENISA is open to new suggestions, and the NLO network is also free to set up its own working groups. It was noted by ENISA that, at present, due to data protection rules, it is not possible to disclose to the MS which experts from their countries are on the groups, or their organisational affiliation, but that a procedure to this effect may be a possibility in the future. The Chair also outlined the ENISA procurement projects foreseen in 2018 and opened the floor for comments and questions from the NLOs. NLOs requested information regarding the policy in place on the affiliation of experts who take part in the ENISA expert groups.

It was indicated that it would be worthwhile to know what publications are expected throughout the year, in order to avoid duplications. In response, ENISA informed the NLOs that this is not always sufficiently clear at the beginning of the year. When the WP is finished, there is only a short time to produce a version of the next one.

Action: All NLOs to liaise with relevant national stakeholders on the information provided by ENISA on expert groups and procurement projects for 2018 before 13 March 2018 (next MB meeting is on 14-15 March and it would be preferable that relevant input exists before that meeting).

Any other business

Under any other business, positive feedback was provided on ENISA's infonotes. It was emphasised by ENISA that these notes are structurally oriented and that ENISA's work is complementary to that of the CSIRT community.

Comments were provided by AT on the NLO Guidelines adopted by the MB in 2017. In particular, AT welcomed the emphasis on avoiding duplication and the two-way information stream and enquired about the existence of a plan regarding updating the guidelines. Some issues that were raised were the distinction between ENISA experts and national experts, and the inconsistency of terminology, particularly NIS vs. cybersecurity. The Chair requested that these comments be submitted in writing.

The date of the next meeting was discussed and September, one month in advance of the Ordinary MB meeting, was identified as a potential date for the meeting as no objections were raised to this date. A physical meeting was preferred over a virtual meeting after a vote by show of hands.

NO	ITEM	ACTION	DEADLINE
1	Introduction by the Chair		
2	Update on the activities of the NLO network and adopted guidelines of operation	*1) NLOs share information on relevant NIS developments in the MS with ENISA PoC*	*Ongoing*
		2) NLOs to provide input to ENISA PoC to prepare report for ordinary MB Meeting	*Before second 2018 NLO meeting*
3.	Tour de table, NLOs	*Inform ENISA on involvement in ECSM and ECSC.*	Continuous
4.	Update on the implementation of the NISD		
5.	EU Cyber Security Act: Certification		
6.	Update on NCSS - activities		
7.	New Awareness Raising Portal on MS Activities	*ENISA to share proposal on Awareness Raising Portal*	*Q2 2018*
8.	Polish Proposition about NLO and Update from Poland		
9.	Secure by Default – UK policy review		
10	CCB and Cert.be		
11.	Transposing the NISD in Slovakia		

12.	Discussion on MS contribution to the WP2018	1) *NLOs to provide input to their MB member on the adopted guidelines* 2) *NLOs to liaise with relevant national stakeholders*	*13 March 2018 (before March MB meeting)*
13.	Any other business		
14.	**Date of next meeting**	*September 2018 (TBD)*	