Meeting Minutes ENISA NLO meeting - 29 January 2019

Meeting:	ENISA NLO meeting - 29 January 2019
Location:	Athens, Greece
Date:	27/06/2019
Attendees:	Andreas REICHARD (AT); Dinela KAYTAZKA (BG); Roman PACKA (CZ); Kia Slaebaek JENSEN(DK); Piret URB (SE); Heidi KIVEKAS(FI); Aude LE-TELLIER(FR); Natalie WENKERS(DE); Anita TIKOS (HU); Porleifur JONASSON (IS); Kieran DUANE (IE); Sandro MARI(IT); Juris PAKALNS (LV); Severin NAESCHER(LI); Viktoras PINKEVICIUS (LT); Laurent WEBER(LU); Matthew YEOMANS (MT); Magdalena WRZOSEK (PL); Isabel BAPTISTA(PT); Rastislav MACHEL(SK); Andrés RUIZ VAZQUEZ(ES); Peter WALLSTROM(SE); Gijs PEETERS (NL); Benjamin SHAPS(UK); Theofanis ANAGNOSTOPOULOS
Apologies:	Neophytos PAPADOPOULOS(CY); Mircea GRIGORAS (RO); Damir SUSANJ (HR); Radovan PAJNTAR (SI); Gunn PETTERSEN (NO); Phédra CLOUNER(BE); Anastasios PAPADOPOULOS (Council); Martin SPAET (EC)

Introduction

Steve Purser, Head of ENISA’s Core Operations Department and Chair of the Meeting, welcomed the members of the NLO network. The agenda was approved by the NLOs.

ENISA noted that there are a number of new members who are welcomed to the NLO network, namely for BG, DK, DE, HR, and NL.

Tour de table

A tour de table was made where the attendees of the meeting introduced themselves and the each member of the NLO network provided an update on the situation in their respective Member States.

Some comments that were noted include:

- The SE NLO noted that a cybersecurity action plan is in production by seven national agencies and will be released in a few weeks time.
- The ES commented that the NIS Directive has been transposed in Spain.
- The NL NLO noted that the Dutch National Cybersecurity Centre has acquired a more independent position within the Ministry of Security and Justice.
- The PL NLO also noted that NIS Directive transposition is finished in Poland.
- The AT NLO thanked for the cooperation in relation to the Cybersecurity Act, which was politically agreed during the Austrian presidency.

- The DK NLO noted that there is a new Danish National Cybersecurity Strategy, adopted in 2018.
- The BG NLO noted that the cybersecurity law transposing the NIS Directive was adopted on 13 November 2018 and that secondary law is in production.
- The CZ NLO noted that the NIS Directive has been successfully transposed and that the process of drafting a new national cybersecurity strategy will follow.
- The LV NLO noted that a new cybersecurity strategy is expected in a few months.
- The LU NLO noted that the NIS Directive is in the process of being transposed into national legislation.
- The DE NLO noted that the NIS Directive has been implemented.
- The FI NLO noted that due to a merger with two other agencies, FICORA is now called Traficom.
- The IT NLO noted that NIS Directive transposition occurred in June last year and that OES have been identified.

ENISA’s New Mandate – Cybersecurity Act

Steve Purser provided an update on the new ENISA mandate as included in the draft Cybersecurity Act. It was noted that the proposed Act contains 2 parts: one on the future of the Agency (including a permanent mandate and more resources but also more responsibilities) and one on a European cybersecurity certification framework.

With regard to the Blueprint, Mr. Purser noted the double challenge of developing a crisis management framework and aligning it with other frameworks. The fact that the draft Regulation contains new responsibilities for ENISA was noted and reference was made to post-incident analysis and the need for a different skill set to perform this task.

Mr. Purser also commented on the certification aspect of the draft Regulation, including the foreseen European Cybersecurity Certification Group (ECCG) and Stakeholder Cybersecurity Certification Group (SCCG). It was noted that the proposed certification framework is voluntary and must be transparent and follow a multi-stakeholder approach. It was also noted that there are some aspects (e.g. the use of standards) that still have to be clarified and developed.

A discussion followed where a question was raised regarding the use of *ad hoc* groups and the representation of smaller states among the experts thereof. It was noted that where possible areas to be explored may include Cloud, SOG-IS and IoT, it is the requester who makes the final decision. For details, NLOs were encouraged to contact NLO PoC Katerina Christaki who can bring NLOs in contact with the relevant ENISA staff involved in certification.

Regarding ENISA’s preparedness to participate in the certification process, it was noted that this is a new activity for ENISA, and that it is foreseen to recruit 6 new technical (non-managerial) posts to meet the Agency’s needs in this area.

Another question was raised concerning the SCCG. It was noted that membership will be *ad personam* and that it is likely to consist of representatives from European organisations.

NLO Network: Status Update and Future Role

NLO PoC Katerina Christaki provided an update on the future role of the NLO Network. Ms. Christaki commented on the composition of the network as well as the history of the collaboration of the NLO network as an informal group. It was noted that, with the new Cybersecurity Act, the NLO network is expected to become a statutory group, which means that the Terms of Reference of the group will have to be updated in line with this new role.

Ms. Christaki also provided some statistics on the participation at the NLO meetings. It was noted that there is an average participation of 21-22 out of 34 members and that 50% of members respond on a regular basis.

Some insights were provided into the draft Cybersecurity Act. It was noted that the proposed Regulation has been politically agreed between the European Parliament, the Council and the Commission and that the NLO network is referenced in Recital 15b and Article 20a thereof. It was noted that the draft Regulation provides for one representative to the NLO network only and refers to the need for internal rules of operation, as is the case for other ENISA statutory groups (e.g. MB, PSG).

A discussion followed, where the relevance of the national education points of contact for the NLO network that is referenced in recital 15b was identified as a point for clarification. It was also clarified that, concerning attendance at the NLO meeting, further details may be specified in the rules of operation.

Additionally, the involvement of NLOs in project planning was discussed and it was noted that more information on what ENISA is doing would help NLOs to contribute more. This information is also available in the work programme. ENISA will engage the NLOs in a dialogue on how to maintain regular and consistent contact on these topics with a view to the project lifecycle. In particular, the solution must be dynamic, keep itself up to date, and control scalability.

Regarding the reply rate of NLOs it was noted that a 50% regular reply rate is not shocking *per se*. ENISA noted that some countries may not reply due to a lack of resources.

It was noted that the outcomes of this discussion may serve as an input to the discussion on the new roles and procedures of the NLO network in view of its foreseen statutory role.

European Cybersecurity Challenge

Demosthenes Ikonomou (ENISA) gave an overview of the Agency's activities in relation to the European Cybersecurity Challenge (ECSC). Mr. Ikonomou explained that the project was first initiative under the umbrella of the 2013 EU Cybersecurity Strategy and outlined the goals and target industries of the ECSC.

Mr. Ikonomou noted the gradual increase in attendance at the ECSC and enumerated some of ENISA's contributions, including its involvement in establishing a governance structure and creating a common platform. It was noted that the 2019 ECSC Final will take place in Bucharest, Romania and that 17 participating countries have confirmed to date.

Training in Information Security Management

Fabio Di Franco (ENISA) provided a presentation on ENISA activities in relation to training in information security management systems (ISMS). Mr. Di Franco introduced some of ENISA's activities in cyber education and training, including online trainings for cybersecurity specialists on the ENISA website, the ENISA-FORTH NIS Summer School and *ad hoc* on-site trainings provided on request of Member States and EU institutions. Mr. Di Franco then provided further details in relation to online training materials aimed at increasing the information security capacity in the public sector and improving CIS skills of civil servants.

NISD Cooperation Group

Konstantinos Moulinos (ENISA) and Marnix Dekker (ENISA) gave an overview of ENISA's activities in support of the NIS Directive Cooperation Group. It was explained that ENISA is involved4 through its work programme and may assist the Cooperation Group on the basis of Article 14 requests. Reference was made to the Cooperation Group report on cooperation which underlined the value of ENISA's support. The presentation also provided an overview of ongoing and future work of the Cooperation Group.

Regarding the involvement of NLOs in the Cooperation group, it was noted in the discussion that ENISA is not involved in the governance structure and that any involvement would have to be routed through the Group itself. It was agreed that ENISA will clarify internally and follow up on this topic.

European Cybersecurity Month (ECSM)

Vangelis Stavropoulos (ENISA) provided an update on the European Cybersecurity Month (ECSM). It was noted that there has been a marked increase in the number of activities associated with the ECSM, the number of twitter followers and the number of articles mentioning the ECSM.

Emphasis was placed on the value of the ECSM evaluation as a feedback mechanism, and it was noted that any comments on this topic may be submitted to the NLO PoC. It was also noted that NLOs can expect a reminder from the NLO PoC concerning the ECSM evaluation.

EU Cybersecurity Act – certification

Andreas Mitrakas (ENISA) provided update on the certification aspects of the draft EU Cybersecurity Act. Mr. Mitrakas described some of the key certification tasks assigned to ENISA in the context of the Act, including the preparation of candidate schemes and review of existing ones, the maintenance of an information portal, supporting peer review between national cybersecurity certification authorities, and the Agency's role with respect to the European Cybersecurity Certification Group (ECCG) and the Stakeholder Cybersecurity Certification Group (SCCG).

Public-Private cooperation in the Netherlands

The Dutch NLO described the approach to public-private partnerships in cybersecurity in the Netherlands. The Netherlands has a decentralised nationwide network of cybersecurity partnerships, which includes 18 Information Sharing and Analysis Centres (ISACs) involving more approx. 300 organisations. In this respect reference was made to the ENISA report on ISACs, as well as the Dutch guide on how to set up an ISAC.

The Dutch NLO also referred to a network of sectoral CSIRTs which aims at the real-time sharing of information, as well as the practice of regional ecosystems. A number of challenges were identified including:

1) the challenge of designing information infrastructure with a feedback loop;
2) cross-sectoral and cross-border sharing of information;
3) increasing the analytical aspect of ISACs;
4) balancing regulation and self-regulation;
5) Looking into supply chain dependencies and increasing resilience.

In the discussion the relationship between CSIRTs and ISACs was clarified in particular that these form separate entities where ISACs typically meet 6-8 times a year. It was also noted that the cooperation in ISACs still typically occurs through traditional means (i.e. meetings).

ENISA also took note of the proposal to convene a working group on the new Terms of Reference. Six NLOs expressed interest at the meeting. It was agreed that ENISA will follow up with an email and NLOs will have a certain amount of time to respond.

Cyber Security for Consumer Internet of Things

The UK NLO provided insights into the topic of cybersecurity for consumer IoT. It is estimated that there will be 12.9 billion consumer IoT devices by 2020, which contributes to the relevance of the topic as poorly secured devices may threaten privacy, online security and safety and can be misused for DDoS attacks.

The UK NLO particularly focused on the new Technical Specification (TS) 103 645 that was approved by ETSI TC Cyber on 18th January 2019 and is scheduled to be published in February. The TS contains 37 requirements and recommendations divided into 13 sections.

The UK NLO explained that the initial draft was based on the UK Code of Practice for Consumer IoT Security and that it offers flexibility as IoT technology develops, is focused, and applicable to all internet connected consumer products and has some industry recognition.

On the basis of these features, the UK NLO suggested that it may form an interesting standard to look at in the context of the draft EU Cybersecurity Act.

Iceland – National developments

The IS NLO provided an overview of national developments in Iceland. By way of introduction, it was noted that CERT.IS is part of the Telecom NRA of Iceland and consists of team of three. Regarding the NIS Directive, the IS NLO noted that the law is approved by the Cabinet, but still needs to go through Parliament, with an expected date of implementation of January 2020.

It was also noted that preparations for assuming a CSIRT role are underway, that planning and preparation of the NIS implementation is taking place, and that an expansion of the CERT team over the next years is expected. The IS NLO referred to the revision of SOPs and operations in conjunction with the FIRST application and noted that Iceland is expecting to be accepted into the FIRST community soon.

The IS NLO provided further details regarding the constituency of CERT.IS, as well as its role in collaboration with law enforcement. It was also noted that Iceland is working on the construction of a nation-wide scanning platform, in cooperation with Syndis, an Icelandic security firm. In particular, the platform will be used to do scanning of IP addresses.

In the discussion, it was explained that Icelandic police do not have a CERT and that there is also no military CERT in place as Iceland does not have an army. It was also noted that one aspect of cooperation with the cybercrime unit is learning to what extent information sharing is possible.

Hungary – National Developments

The HU NLO provided a presentation on national developments in Iceland. An overview was provided of the organisational structure of cybersecurity in Hungary, where a differentiation was made between the strategic and operational level, and both fall under the Ministry of Interior. It was noted that the National Cybersecurity Centre is the PoC for EU-related topics.

An update was provided on the implementation of the NIS Directive in Hungary and it was noted that implementation is taken place but not yet completed. The HU NLO referred to the Hungarian National Cyber Security Strategy adopted in 2013 and explained that this strategy does not meet NISD requirements by itself. Accordingly, the government has adopted the Hungarian National Strategy for NIS Systems Security (sectoral) to fulfil NISD requirements with an action plan until 31st March 2019.

It was also noted that Hungary has transitioned from “GovCERT” to National Cybersecurity Centre.

Following this presentation, ENISA announced that a written request will be made regarding the upcoming Industry Event on 1st March 2019 and that ENISA would appreciate any input regarding potential speakers.

Discussion on MS contribution to the WP2019

A discussion took place regarding the outputs of the ENISA Work Programme 2019 where presentations were provided by the Heads of ENISA’s operational units and teams, followed by questions and answers.

COD 1 – Secure Infrastructure and Services

Evangelos Ouzounis (ENISA) presented the activities of the ENISA Secure Infrastructure and Services Unit (COD 1) starting with O.1.1.1, Good practices for Security of IoT. Mr. Ouzounis informed the NLOs of a deliverable in the form of secure software development guidelines and the planned ENISA-Europol Conference on IoT Cybersecurity was also noted. Two expert groups were referenced, namely the IoT Security Expert Group and the ENISA ICS Stakeholders Group.

In relation to the IoT expert group it was noted in the discussion that this group is very popular has 18-20 people, has probably reached saturation and that there are no current plans to publish a new call in this area. In relation to the role of the Member States, it was noted that some Member States are represented in expert groups, and involved in validation workshops and stocktaking providing an opportunity for Member States to be involved and provide feedback.

Mr. Ouzounis gave an overview of the COD 1 activities under O.1.1.2, Good practices for Security of Smart Cars, noting deliverables in relation to Vehicle2Vehicle communication and infrastructure. The smart cars security workshop was also mentioned, as well as support to the Commission, Member States and automotive industry. Mr. Ouzounis also mentioned the CARSEC expert group.

An overview was provided of the COD 1 activities under O.1.2.3 with regard to supporting incident reporting in the EU, with reference to the work in relation to Article 13(a) of Directive 2009/140/EC and Article 19 of the eIDAS Regulation. Reference was made to the Article 13(a) and Article 19 expert groups. Mr. Ouzonis also addressed Output O.2.2.2 on ENISA's work supporting the implementation of the Work Programme of the Cooperation Group, referring the Cloud Security expert group, as well as the Article 19 expert group. It was noted that an email will be sent to the NLOs in the event of a new call for applicants for the Cloud Security expert group. In relation to the Cooperation Group it was noted that ENISA itself only has a supporting role, and that the governance structure is controlled by the Commission. Mr. Ouzounis also provided an overview of the activities of COD 1 in relation to assisting Member States In the implementation of OES and DSP security requirements, Output O.2.2.3.

A discussion occurred where it was noted that knowing when stocktaking exercises are launched would be very helpful for NLOs. ENISA noted that projects are started with a stocktaking of 2-3 weeks, where NLOs will be approached by ENISA. It was also noted that draft reports should usually not be shared with third parties and that validation workshops are open and allow for input from a broader range of stakeholders.

Mr. Ouzounis also provided an overview of COD 1 activities in relation to supporting the Payment Services Directive implementation (O.2.2.4), supporting the implementation of the Electronic Communications Code (O.2.2.7), and supporting EU Member States in the development and assessment of National Cybersecurity Strategies (O.3.1.2). In relation to the final output, the NCSS Workshop in Warsaw in cooperation with NASK was noted, and an explanation was provided of the NCSS evaluation tool.

COD 2 – Data Security and Standardisation

Andreas Mitrakas (ENISA) provided an overview of ENISA's activities in the Data Security and Standardisation Unit (COD 2). Mr. Mitrakas explained ENISA's activities in relation to discussions in the area of certification, Output O.2.1.1, referring in particular the SOG-IS expert group. Mr. Mitrakas also noted ENISA's work in supporting the preparatory policy discussions in the area of certification.

Mr. Mitrakas also described COD 2 activities in contributing to EU policy in the area of privacy and data protection with policy input on security measures, Output O.2.2.5, referring to two expert groups in this area. Additionally Mr. Mitrakas provided some background on COD 2's work in relation to the Guidelines for European Standardisation in the field of ICT security, Output O.2.2.6 and supporting the fight against cybercrime and collaboration between CSIRTs and Law Enforcement Agencies, Output O.4.2.2.

Mr. Mitrakas also referred to three procurement projects, namely an ENISA business model and public website on cybersecurity certification, and two recommendations in relation to the eIDAS Regulation.

A discussion ensued where the Common Criteria (CCRA) were featured. It was noted that ENISA adopts a balanced point of view, and is interested in a number of existing frameworks that are in place, including the CCRA and the New Legislative Framework, where the final outcome regarding the choice on the kind of certification projects that will be pursued lies with the Commission and the Member States.

COD 3 – Operational Security

Demosthenes Ikonomou (ENISA) provided an overview of ENISA's activities in the Operational Security Unit (COD 3). Mr. Ikonomou referred to COD 3's activities under Output O.1.1.3 in relation to cryptography and the ECRYPT-CSA action. Mr. Ikonomou also mentioned Output O.3.3.1 and COD 3's work on Cybersecurity Challenges and the associated expert group. Finally, Mr. Ikonomou referred to Outputs O.4.1.1 and O.4.1.2, and the group that represents the EU Member States participating in the Cyber Europe Exercise.

It was noted in the discussion that each country that participates in the European Cybersecurity Challenge has its own right to select who coordinates the national challenge.

CR – CSIRT Relations

Andrea Dufkova (ENISA) provided an overview of ENISA's activities in the CSIRT Relations Team, noting in particular procurement projects under Outputs O.3.1.1, O.3.1.3 and O.4.2.1. Ms. Dufkova also referred to the technical trainings expert group and incident response expert group.

HAS – Horizontal Support and Analysis

Steve Purser (ENISA) presented the activities of ENISA in the Horizontal Support and Analysis Team. Mr. Purser referred in particular to the European Threat Landscape Report and the associated expert group, as well as ENISA's delivery of info notes with a long-term vision.

MeliCERTes

It was noted that ENISA is expected to run the central hub of the MeliCERTes platform.

AOB

Some further information was requested regarding the MoU between ENISA, EDA, CERT-EU and Europol's EC3. ENISA explained that the cooperation envisaged has synergies with the WP and referred to activities with regard to cyber exercises where EDA takes the lead, as well as trainings and exchange of expertise.

In relation to project planning it was noted that ENISA provides input to the NLOs in this area, at the beginning of the year through its annual meeting.

ENISA also provided some background information regarding ENISA's 15 years anniversary event.

The date of the next meeting will depend upon the formal adoption of the CSA and it is expected to take place in Q3/Q4 2019.