Council of the
European Union

Brussels, 31 October 2018
(OR. en)

13810/18

CYBER 257	**POLMIL 190**
COPEN 373	**RELEX 921**
COPS 395	**TELECOM 372**
COSI 247	**DAPIX 339**
DATAPROTECT 234	**CATS 79**
IND 316	**CSC 303**
JAI 1088	**CSCI 143**
JAIEX 148	**IA 346**

NOTE

From:	General Secretariat of the Council
To:	Delegations
No. Cion doc.:	12104/18
Subject:	Publication of the EE-BG-AT Trio Presidency Cybersecurity Work Programme

On 30 June 2017, Estonia, Bulgaria and Austria tabled the Trio Presidency Cybersecurity Work Programme which defines common goals and concrete actions up until the end of 2018 for building strong cybersecurity in the EU.

This Work Programme was framed by the perception of the crosscutting, cross-sectoral and cross-border character of cybersecurity on the one side, and on the other side of the special, strong role of Member States in their prerogative of national security and consequently the need for a proactive approach in the Council work. At the end, the chain is as strong as the weakest link and therefore the cyber resilience of each Member State as well as of the EU intuitions, agencies and bodies is a crucial precondition for our democracy and the functioning of the Digital Single Market.

The Work Programme itself has special symbolic meaning as for the first time three Member States have decided to express their collective commitment in cybersecurity as a political act in the form of a dedicated work programme for 18 months. This step was aimed to contribute to the transparency and accountability of the policy making process in times when cyber risks permeate all aspects of our lives. The process that led to the Trio Presidency Cybersecurity Work Programme is result of intensive trilateral negotiations and represents a whole-of-government of commitment for enhancing the EU cybersecurity and resilience on political, strategic and operational levels. In light of the need for a proactive role of the Council in cybersecurity, the trio programme was also created in full accord with the Cybersecurity Package put forward by European Commission on 13 September 2017, and other developments, but also setting own initiatives.

The implementation of the Trio Presidency Cybersecurity Work Programme was a shared goal for Estonia, Bulgaria and Austria and it has progressed very well with many achievements on the side of the Council. Austria being the third in the line is committed to fulfil the remaining initiatives and to take stock by the end of its Presidency.

The idea of a devoted middle-term programme on cybersecurity over 18 months was welcomed by the Member States in terms of continuity and also helped as a valued planning tool to structure the work of the Presidencies. Therefore, it is a common recommendation of the current Presidency Trio to the upcoming Trios to follow this example and to create their work programmes which would not only be reactive but also proactive to common initiatives or actions, evaluating and reflecting on those of the previous Presidency Trios.

Committed to full transparency and accountability, the EE-BG-AT Trio Presidency has decided to publish the Trio Presidency Cybersecurity Work Programme as presented to the Horizontal Working Party on Cyber Issues on 3 July 2017 [*](Annex).

[*] The text is identical to doc. WK 7101/2017.

Cybersecurity programme of the EE-BG-AT trio Presidency

At the start of the EE-BG-AT trio Presidency in July 2017, the EU is at the point where cyber risks and cyber-attacks challenge, among other things, the very nature of our democratic processes, our essential services and infrastructure and weaken the trust in our digital economy. Thus, the importance of well-developed cybersecurity systems and culture in the EU and in the Member States (MS) has risen to an entirely new level. The weakening of public trust in the Digital Single Market (DSM) has a clear and direct economic impact on the Union as a whole. The strengthening of the European cybersecurity industry and the reduced dependencies on security technologies developed outside the EU are of great importance in this context. As a result, the trust in democracy and in our digital economy and our economic growth as a whole depend on adequate and effective cybersecurity in MS and the EU. To cope with these challenges, the upcoming trio Presidency has agreed upon the following cybersecurity programme for the next 18 months. This programme covers the activities of the Horizontal Working Party on Cyber Issues (HWP Cyber) in the Council, on the one hand, and the NIS Cooperation Group (NIS CG) and the CSIRTs Network, on the other. The trio Presidency wants to ensure that these groups work and function complementarily and to avoid unnecessary duplication. The trio Presidency will be guided in this work by two principles: the whole-of-government approach and the inclusion of the private sector, academia and civil society views where needed. The trio Presidency is aware that the Cyber trio programme touches only upon few aspects of the cybersecurity ecosystem and further changes as well as adaptations might also be necessary in every respective national programme of the trio Presidency. The topics and the elements which the trio Presidency wants to observe and address in the course of the next 18 months are however elaborated below. They are crucial for the improvement of the awareness and robustness of the MS and the EU.

1) Developing the EU strategic vision for cybersecurity and the renewal of the EU Cyber Security Strategy (EUCSS): In the second half of 2017 the EU will renew its Cybersecurity Strategy. The trio Presidency will seek to consolidate the views of the MS in the Council on that matter. The renewal of the strategy will serve as an opportunity for the EU to stand up and respond to the challenges posed by cyber risks, deliver strategic messages for increasing the trust in the DSM and communicate globally its core values for cyberspace. The trio Presidency has a clear common understanding that the misuse of cyberspace and/or of cyber tools to undermine democratic processes in the EU will not be tolerated and has to be met with an adequate European response. Reducing systemic threats and strengthening resilience is key in this context. At the same time, the renewal of the EUCSS will serve as an opportunity for the MS to reinforce their cybersecurity commitment. This will be a good opportunity to develop a common vision for cybersecurity among MS in the Council. Depending on the content of the new EUCSS, the trio Presidency aims to use this either to reflect on the EUCSS vision or to start a process for developing this vision in the next 18 months and review the progress by the end of the trio. The trio Presidency will work towards the adoption of Council conclusions on the renewed EUCSS 2017, building on the outcomes of the EUCSS 2013 and taking into account the Roadmap (doc. 8901/17 of 11.5.2017). Along with that, the trio Presidency considers the implementation of the new EUCSS to be overseen by HWP Cyber. Therefore, the trio Presidency will table an action plan for the EUCSS 2017 which HWP Cyber will regularly review and update, based on the principles, objectives and measures laid down in the EUCSS 2017.

2) Implementation of the NIS Directive: A strategic priority for the trio Presidency is to support the full and timely implementation of the NIS Directive (NISD). The NISD is the first legislation for cybersecurity at EU level and establishes a legal basis for creating a level playing field on cybersecurity in the MS, and therefore it should be implemented in close cooperation between the European Commission and the MS. The successful implementation of the NISD across the MS is one of the preconditions for trust in the DSM and its functioning. To support this goal, the trio Presidency will:

a. ensure the substantial work of the NIS CG in all its current work streams – from essential services to cross-border dependencies. In order to provide the NIS CG with a long-term vision, the trio Presidency will propose a biennial work plan in line with the NISD, but will also lead discussions on strategic matters among the MS in the NIS CG. The Presidency trio will ensure also sufficient strategic direction from the NIS CG to the CSIRTs Network by providing a strong link between the two groups.

b. ensure the development of the CSIRTs Network as the EU-wide confidence and trust building operational platform among the CSIRTs of the MS and as the basis for achieving better situational awareness on part of MS regarding the current risks and responding to threats in cyberspace. In order to ensure that this vision is fulfilled, adequate technical means and tools have to be put in place to carry out activities that facilitate a greater openness and cooperation between the CSIRTs and which achieve a level playing field in terms of their cybersecurity capabilities and practices.

3) Cyber Diplomacy: A trio Presidency priority is to finalise the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities. This will bridge the gap between shared situational awareness and the political decision-making including actions at EU level. In order to make this Framework a political tool for prevention, mitigation or discouragement of malicious cyber-activities against MS and EU institutions, the Framework will have to be accompanied by clear implementing guidelines, solid preparatory practices and communication procedures. This could be only achieved by a clear EU institutional cyber map with a clear understanding of the respective roles and responsibilities. This would help to avoid confusion during a time of crisis especially if the respective procedures are practised regularly by the MS and the EU institutions. The trio aims to finalise the discussion on the Framework during the EE Presidency and to prepare and conduct a Cyber Diplomacy Exercise on the Framework activation during the BG and AT Presidencies, planned for 2018. Besides that, the preparations of cyber dialogues with third countries and cooperation with relevant international and regional organisations (e.g. OSCE, NATO, UN, CoE) will continue to be part of the regular work of HWP Cyber.

4) ENISA 2.0: By providing ENISA with a new mandate, the trio Presidency will ensure that the new ENISA adds value by fully respecting the MS' competences and capabilities and build its work on those. The new ENISA should assist the MS in their implementation of the NISD, support the CSIRTs network and develop it further as well as assisting the work of the NIS CG as required in the NISD. It should complement all this with an adequate exercise programme. To this end ENISA will need to further develop, deepen and specify its performance portfolio and it will also need to be provided with sufficient access to human and financial resources. Having a permanent presence in Brussels would bring ENISA closer to EU political decision making and would strengthen the relevance of ENISA within the EU cyber map. The negotiation of the ENISA mandate will be the first negotiation of a legislative act in HWP Cyber and this will be of importance for in further functioning of HWP Cyber.

5) Standards / certification / label / trusted supply chain: The EU will have to take some clear steps to reduce its dependence on security technologies developed outside the Union. Based on the work done so far by ECSO and taking an inclusive approach towards all MS and their potential as a basis, the trio Presidency prioritises the EU's work towards gaining a leading role in developing the next generation digital technologies, evaluating the security of digital products and solutions and reducing the dependency on foreign security technologies. This work will be also aimed at achieving a security-by-design approach taking into account all relevant EU policies and programmes.

a. Cybersecurity certification framework: the initiative is expected to be launched by the European Commission in the second half of 2017 and will have a huge potential for achieving several security targets related to cybersecurity. In order to maximise this potential, the initiative will have to be inclusive and take into account global standards and certification schemes, ensure equal participation opportunities for all MS and flexible inclusion of different digital products and services as decided by the MS. The trio Presidency will start its work and its deliberations on this framework as soon as it is presented by the European Commission.

b. European crypto policy: The lack of a common European framework for cryptographic algorithms and protocols has been a concern in view of the dominant market position of some non-EU states. It is of the utmost importance to develop European competences and capabilities to evaluate the cryptographic aspects of the digital products and services used by citizens, businesses and governments within the Single Market. Therefore a European crypto policy has to be a major item on the agenda of the Cybersecurity community, and it must be accompanied by technical procedures and documents by the industry.

c. Research & development in general: the discussion of the current and future challenges should be considered as an inherent part of the work on cybersecurity. The trio Presidency aims to bring together the results and the findings from other areas in order to discuss them, especially in HWP Cyber, and address Next Generation technology challenges in the context of Cybersecurity.

6) Cybersecurity capacities and cyber resilience of the Member States: the strengthening of the cybersecurity capacities of the MS and the consequent strengthening of their cyber resilience are essential in order to provide a high level of network and information security throughout the MS (keyword capacity building in the EU). Taking into account the importance of this topic, the trio will take concrete measures in order to provide MS with a clear picture of the status quo:

a. discussion on Training & Education and practical application in order to address the lack of cyber experts in the EU;

b. promote the usage and development of Cyber Ranges in providing MS and the EU with a

robust cyber exercise programme;

c. voluntary assessment of the robustness of MS in the face of cyber threats based on already existing work (ENISA, CSIRTs network) and questionnaires in the CSIRTs network and the NIS CG, as well as identification of strengths and deficiencies (voluntary consultations with MS) with the support of ENISA (e.g. lessons learned);

d. Council Conclusions in HWP Cyber on the basis of the results of the questionnaires in the CSIRTs network and NIS CG defining the potential for improvement: what capacities will be needed, what is not yet finished, what is not yet implemented, what is still needed and what common steps are necessary next.

7) Cyber resilience of the EU Institutions and clarity on the European institutional cyber map: In

order to prepare the EU to deal with future large-scale cyber-attacks, the trio will work towards ensuring that MS have a clear picture of and sufficient information on the responsibilities and roles of the different EU institutions, agencies and bodies in cybersecurity and will try to make the cooperation between them and their different groups work more seamlessly. A clear European institutional cyber map is also a requirement for the functioning of the Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities. Besides creating conditions for strengthening the cyber security of the MS, the EU will also have to ensure that its own networks and systems are properly protected and well prepared in the event of a large scale cyber-attack against the EU institutions, agencies and bodies. The cyber resilience of CSDP missions and operations is also very important for the trio Presidency, therefore, the EE Presidency will conduct a table-top exercise during the informal Defence Council. All this should encompass both commitment and investment on the part of the EU institutions in cyber security, but it should also provide grounds for ensuring better situational awareness among the MS. The trio Presidency is aware of the fact that ensuring cyber resilient EU institutions lies within the competences of the EU institutions themselves but taking into account the importance for the functioning of the EU and their contribution to a better situational awareness among the MS, the trio Presidency wants to support this process through the following measures:

a. given the necessity for a better and clearer cyber map at EU level, the trio will make efforts to map all existing EU and European groups/initiatives (living document with contributions from MS and EU institutions, agencies and bodies) in order to understand what is already happening, what is the level of cooperation, how the respective decisions are taken within these groups and initiatives and how do they correlate with one another, what their results are and how relevant they are for HWP Cyber;

b. provide regular situational snapshots of the threats against the EU institutions (CERT EU) to foster a common understanding of the cyber threats at EU level;

c. develop synergy between the bodies dealing with Cybercrime, Cyberdefence and Cybersecurity and their communities.

8) Cybersecurity industry and Cyber PPP model: The trio Presidency underlines the importance of the cybersecurity industry and the inclusion of economic, academic and civil society actors and in this regard, the fostering of the Cyber PPP models at EU level will also be on the agenda in the next 18 months. On the one hand, the trio wants to ensure a regular link between ECSO and HWP Cyber. On the other hand, the trio wants to assess the effectiveness and the work of ECSO since its creation, analyse other PPP models and work out, whether all aspects of a PPP are covered by ECSO. The results of this examination should lead to the necessary measures being taken: optimisation, adaptation or expansion of the ECSO.

9) Criminal Justice in cyberspace: Emphasising the application of international law, fundamental rights and freedoms as the basis for increased security in cyberspace, the co-operation of MS in attributing cyber-attacks and in identifying and prosecuting the perpetrators is critical for the trio Presidency in order to be able to respond to the clear challenge posed by cybercrime. The trio will follow the ongoing work on improving enforcement of jurisdiction in cyberspace within the framework set out by the GDPR, the NISD, and the Data Protection Directive for Police and Justice and other relevant instruments. Ensuring quick access to electronic evidence in criminal investigations is instrumental and the trio Presidency will monitor and guide the discussion on eevidence organised by the COM in a follow-up to the June 2017 Council with a view to the implementation of the identified practical and legislative measures for improved cooperation among government authorities and with service providers. As telecommunications data is crucial for investigating terrorism, and other serious crime, including cybercrime, the trio Presidency will follow the work of the FoP DAPIX/Data Retention towards a common EU position to improve enforcement of jurisdiction in cyberspace in a way that respects the fundamental rights granted by the European Charter and interpreted by the ECJ through the setting high standards, especially the right of data protection and privacy. The trio Presidency will advance discussions on the role of encryption in criminal investigations, noting that while encryption poses challenges for the law enforcement authorities, strong encryption enables development of safe digital solutions and e-services and is a basis for citizens´ trust in the Digital Single Market as a strong privacy and data protection tool. The trio Presidency will examine ways to improve EU´s capacity to fight cybercrime, notably by strengthening Europol´s European Cybercrime Centre (EC3), and by making better use of EU research funds. The trio will also follow the work of the relevant Council preparatory bodies, e.g. FoP Hybrid Threats and FoP Interoperability and will avoid unnecessary duplication.

10) Roles, linkages, and communities: A synergy between HWP Cyber, on the one hand, and the NIS CG and CSIRTs network, on the other, should be sought (including regular briefings provided to HWP Cyber, taking into account the its coordinating, strategic and horizontal character. Furthermore, the trio will aim to continue and deepen the cooperation and information exchange between the various cyber communities, e.g. cybercrime, cyber justice, cyber diplomacy and cyber defence and the synergies between them. The exchange with the Cybercrime and Cyber Justice communities is already taking place within the framework of HWP Cyber, thus the trio will also work to strengthen the exchange with the rest of the cyber communities, in particular the Cyber Defence community.

The trio Presidency is aware of the utmost importance of cybersecurity and its cross-border character and its complexity in the context of the structures, competences and topics concerned. It is also aware of the challenges and various questions arising from it. Our programme represents an attempt to address these challenges and questions in order to strengthen the preparedness and the resilience of the EU and the MS during cyber-attacks. For this purpose, the trio Presidency will seek support and consensus from all MS and EU institutions because only together are we strong!