Council of the European Union

Brussels, 21 September 2022
(OR. en)

11237/2/22
REV 2

LIMITE

CYBER 262
TELECOM 327
COPEN 283
COSI 202
DATAPROTECT 223
IND 294
RECH 444
HYBRID 80
JAI 1043
POLMIL 178
RELEX 1026

NOTE

From:	Presidency
To:	Delegations
Subject:	Draft Council conclusions on ICT supply chain security

Delegations will find in the Annex a revised draft of the Council conclusions on ICT supply chain security following the discussions at the HWPCI meeting on 16 September 2022 and comments received afterwards. The draft will be submitted for discussion to the Horizontal Working Party on Cyber Issues on 23 September 2022.

Draft Council conclusions on ICT supply chain security

THE COUNCIL OF THE EUROPEAN UNION,

RECALLING its conclusions on

– the Joint Communication of 20 November 2017 to the European Parliament and the Council: "Resilience, Deterrence and Defence: Building strong cybersecurity for the EU"[1],

– cybersecurity capacity and capabilities building in the EU[2],

– the significance of 5G to the European Economy and the need to mitigate security risks linked to 5G[3],

– shaping Europe's Digital Future[4],

– "A recovery advancing the transition towards a more dynamic, resilient and competitive European industry"[5]

– the cybersecurity of connected devices[6],

– the EU's Cybersecurity Strategy for the Digital Decade[7],

– the development of the European Union's cyber posture[8],

– the Special Report No. 03/2022 by European Court of Auditors entitled „5G roll–out in the EU: delays in deployment of networks with security issues remaining unresolved"[9],

1 14435/17 + COR 1
2 7737/19
3 14517/19
4 8711/20
5 13004/20
6 13629/20
7 6722/21
8 9364/22
9 9616/22

RECALLING the European Council Conclusions on

– COVID-19, the Single Market, industrial policy, digital and external relations of 1-2 October 2020[10],

– Russian military aggression against Ukraine, security and defence, energy, economic issues, Covid-19 and external relations of 24-25 March 2022[11],

– Ukraine, food security, security and defence and energy of 30-31 May 2022[12],

1. Given the increasing relevance of geopolitics for cybersecurity, EMPHASISES that the European Union and its Member States need to approach cybersecurity in a comprehensive and strategic manner. Russia's military aggression against Ukraine has caused a major shift in the European Union's strategic and security environment and has shown the need for a stronger and more capable European Union in the field of security and defence. It has highlighted that it is of utmost importance to appropriately take the geopolitical environment into consideration not only when reacting to malicious cyber activities, but also when building and maintaining the resilience of information and communication technologies (ICT). This is of special relevance for supply chains of ICT products and services (ICT supply chains), which might be both compromised on the basis of geopolitical rivalry, as illustrated by the SolarWinds attack, and affected by geopolitical tensions and instability, as shown by the threat related to the dependence on Russian ICT vendors at the time of Russia's military aggression against Ukraine.

10 EUCO 13/20
11 EUCO 1/22
12 EUCO 21/22

2. NOTES that the character of the risks associated with ICT supply chain, which is composed of a linked set of resources and processes between economic operators (as defined in Regulation (EU) 2019/1020) that begins with the sourcing of raw material and extends through the manufacturing, processing, handling and delivery of ICT products and services, including provision of support during ICT products and services' life cycle, brings unique challenges and potentially far-reaching consequences. Besides the risks related to the unavailability of ICT products, for instance, due to shortages of critical raw materials and semiconductors needed for their production, the supply chains of ICT products and services are exposed to other threats. Notably, they may be targeted or misused by malicious actors in sophisticated, often concealed, ways that have impacts on the confidentiality, integrity and availability of transmitted and stored sensitive data.

3. Recognising that an all-hazard approach is needed in securing ICT assets, ACKNOWLEDGES the relevance of the proposal for the Critical Entities Resilience Directive to improve the physical security of critical entities, and EMPHASISES that in addition to enhancing resilience against supply chain attacks conducted via cyber means, it is equally important to strengthen the overall resilience and security of ICT supply chains against the whole variety of threat factors, such as natural events, system failures, insider threats, or human errors. In this sense, RECOGNISES that ICT supply chain security encompasses **ensuring the** protection of ICT products and services produced**,** ~~and~~ delivered, **procured and used** ~~though~~ **in** ICT supply chains, including ~~the~~ **by means of** ~~protection of~~ **protecting** individual components and transmitted data**.**~~, from any events that have negative effects on their availability, or confidentiality and integrity, where applicable, on economic operators' side, and ensuring an adequate level of security of ICT products and services procured and used on customers' side.~~

4. Drawing on the lessons from the consequences of strategic dependencies of the European Union on Russian fossil fuels as well as from the impacts of the disruptions in supply chains during the COVID-19 pandemics, notably in relation to pharmaceuticals and semiconductors, where the EU's strategic dependencies were exposed, ENCOURAGES Member States to work towards avoiding similar situations of unwanted strategic external dependencies in relation to ICT products and services. Because **of** the growing digitalisation of society and the ever-increasing use of ICTs in critical infrastructure, strategic external dependencies related to ICT products and services and their supply chains should be continuously assessed and, where appropriate, addressed.

5. RECALLS that achieving strategic autonomy while preserving an open economy is a key objective of the Union, which includes identifying and reducing strategic dependencies and increasing resilience in the most sensitive industrial ecosystems and specific areas, including in the digital area. This comprises of developing and deploying strategic digital capacities and infrastructure as well as reinforcing the ability to make autonomous technological choices and as one of the main pillars, ensuring resilient and secure infrastructures, products and services for building trust in the Digital Single Market and within the European society, while maintaining openness, global cooperation with like-minded partners and competitiveness, and harnessing the potential benefits thereof. The European Union's core values preserve in particular privacy, security, equality, human dignity, rule of law and open Internet as prerequisites for reaching a digital-driven human-centric society, economy and industry.

6. NOTES that due to developments in the cyber threat landscape demonstrated by the trend of highly impactful and sophisticated supply chain attacks in recent years, such as SolarWinds, Mimecast, or Kaseya attacks, emerging together with the outsourcing of essential ICT services and intensified by the overall reliance on ICT products and services manufactured, provided, or serviced by third parties, the occurrence of more supply chain attacks with substantial damage to the economy and society is in the future highly likely. In view of this, EMPHASISES the importance of enhancing the security and resilience of ICT supply chains for the functioning of the Single Market ~~as well as~~ **together with** the need to ensure the availability**, security** and diversity of ICT products and services in the Single Market. Therefore, ACKNOWLEDGES the need to maximise and streamline the use of existing EU instruments and approaches to achieve these objectives as well as the need to continually adapt to the changing cyber threat landscape by introducing additional suitable measures and mechanisms, including in relation to **possible security risks of** emerging and disruptive technologies. **ENCOURAGES Member States to pursue in this regard the risk-based approach to tackle new technology developments.**

7. ACKNOWLEDGES that understanding the constantly evolving cyber threat landscape as well as the complexity of supply chain attacks is essential for the effective mitigation of risks associated with ICT supply chains. In this regard, STRESSES the necessity to **adjust to new threats by actively and** continually ~~monitor, analyse, and assess~~ **monitoring, analysing, and assessing** the supply chain threat landscape**,** to raise awareness and build knowledge **about threats and vulnerabilities, and to proactively alert relevant entities in a tailored manner.** ~~in order to adjust to new threats and~~ WELCOMES the work of **the European Union Agency for Cybersecurity (**ENISA**)** related to ICT supply chain security, particularly its Report on the Threat Landscape for Supply Chain Attacks.

CROSS-SECTORIAL INSTRUMENTS AND APPROACHES

8. REAFFIRMS the importance for Member States to consider the need to diversify suppliers of critical ICT in order to avoid or limit the creation of major dependencies on single suppliers, and in particular high-risk suppliers, as it increases the exposure to the consequences of potential disruptions. RECOGNISES the avoidance of vendor lock-in and the diversification of ICT suppliers as one of the important components for ensuring stability and security of the internal market. HIGHLIGHTS the need of promoting and implementing appropriate strategies facilitating vendor diversification and competitiveness in a technology-neutral manner. In addition, ENCOURAGES integrating aspects related to the prevention of vendor lock-in into EU legislation. In this regard, ACKNOWLEDGES the proposal for a Regulation on harmonised rules on fair access to and use of data (Data Act), aiming to increase the interoperability of data processing services and to remove obstacles to the switching between providers of data processing services.

9. RECOGNISES the link of ICT supply chain security to public procurement. EMPHASISES the need for the ~~legislation on~~ public procurement **procedures** to adequately take into account the importance of ICT supply chain security by providing a sufficient range of means for the **possible** exclusion **– based on objective, risk-based criteria –** of tenderers who may raise doubts about their capability to ensure a high level of security of the provided services. CALLS for finding the right balance between public interest in the most efficient and fair use of public funds on the one hand and the public interest in securing information systems and ensuring the smooth functioning of the Single Market on the other hand. To facilitate the implementation of relevant public procurement rules in light of increasing cybersecurity, INVITES the Commission to develop methodological guidelines by the third quarter of 2023 in order to encourage the contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors, and to assess and, ~~where~~ **if** needed, make proposals to revise or complement relevant public procurement legislation.

10. ACKNOWLEDGES that foreign direct investments related to ICT products and services, while providing economic and social benefits to Member States, businesses and citizens, could include risks to security and public order and NOTES that the EU's Foreign Direct Investment Screening mechanism, along with respective national screening systems, which provide means to address such risks, can also be applied as a useful tool for safeguarding security and resilience of the ICT supply chain by contributing to the elimination of high-risk investments that may affect such security and resilience. STRESSES that information exchanged and shared through this mechanism may help Member States better assess the possible threats to the security of ICT supply chains and take necessary steps accordingly. CALLS on the relevant national actors to also account for this dimension of the screening mechanism, where appropriate.

11. With regard to defence, REAFFIRMS its invitation for the Commission to assess in 2023, together with Member States, the risks for supply chains of critical infrastructure in various domains, including the digital domain, related to the EU's security and defence interests as well as to explore options to increase cybersecurity across the whole supply chain of the EU's Defence Technological and Industrial Base. Furthermore, INVITES Member States and the Commission to reflect on ICT supply chain security in the implementation of the commitments and actions of the Strategic Compass.

12. Recognising the importance of critical raw materials as well as all kinds of semiconductors as the basic building blocks for ICT products, ENCOURAGES ~~swift~~ **constructive** negotiations of ~~future~~ **the Proposal for a** Regulation~~s~~ establishing a framework of measures for strengthening Europe's semiconductor ecosystem~~, namely the future~~ **(**Chips Act**)** and **the Proposal for a Council Regulation amending Regulation (EU) 2021/2085 establishing the Joint Undertakings under Horizon Europe, as regards** the Chips Joint Undertaking.

13. Specifically with regard to telecommunication infrastructure, ACKNOWLEDGES the achievements at the Union level to improve the supply chain security of 5G networks, particularly through the EU Toolbox for 5G security (EU 5G Toolbox). CALLS on Member States to further exchange information on best practices and methodologies regarding the implementation of measures recommended in the EU 5G Toolbox and in particular to apply the relevant restrictions on high-risk suppliers for key assets defined as critical and sensitive in the EU coordinated risk assessments. HIGHLIGHTS that the EU 5G Toolbox represents an agile risk-based instrument to address identified security challenges, which allows handling 5G cybersecurity aspects in a timely and efficient manner, while respecting the competences of the Member States, and RECOGNISES it to be a valuable instrument to further enhance, in full transparency, the supply chain security of telecommunication networks in a coordinated manner that might serve as an inspiration for risk assessment and mitigation tools related to other vital sectors. RECALLS the invitation of relevant authorities to formulate recommendations, based on risk assessments, to Member States and the Commission in order to reinforce the resilience communications networks and infrastructures within the European Union, including the continued implementation of the EU 5G Toolbox.

14. NOTES the importance of ~~open~~ interoperable approaches that can address vendor lock-in and dilute concentration risk, ~~thereby~~ **while** improving supply chain security **across the whole spectrum of ICT infrastructure and services**. Particularly in relation to 5G networks, RECOGNISES the potential benefits of Open RAN concept in that regard, while at the same time **RECALLS the Report on the cybersecurity of Open RAN published by the NIS Cooperation Group noting** ~~NOTES~~ that this concept is still under development and its security**, transparency and standardisation is** at an early phase of maturity**,** and **EMPHASISES the importance to assess risks in advance of any transition towards new standards or architectures**.

15. HIGHLIGHTS the relevance of existing and forthcoming cybersecurity horizontal legislative instruments, notably the **Regulation on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (**Cybersecurity Act**)**, the forthcoming Directive on measures for a high common level of cybersecurity across the Union (NIS2), the Proposal for a Regulation on laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union, as well as the ~~future~~ **Proposal for a Regulation on cybersecurity requirements for products with digital elements (**Cyber Resilience Act**)**, for increasing ICT supply chain security. In addition, NOTES the important developments in sector-specific cybersecurity regulations, in particular the future Regulation on digital operational resilience for the financial sector (DORA), which includes an oversight framework for the ICT third-party service providers that are critical for financial entities. These regulations bring general obligations related to supply chain security as well as detailed and specific requirements relevant for the concerned sector. At the same time, STRESSES that suppliers often supply their products and services across different sectors, rather than to a single industry. Therefore, it is highly important to ensure that the supply chain security requirements are, to the extent possible, aligned throughout all relevant sectors, especially those covered by the future NIS 2 Directive, in order to avoid discrepancies between the obligations imposed on suppliers as well as to ease the burden on operators of critical sectors of assessing the compliance of suppliers with those obligations, while taking into account sector specificities.

16. **WELCOMES the Cyber Resilience Act proposal as an important legislative instrument for advancing the secure development of products with digital elements, and for ensuring cybersecurity is accounted for in the full life cycle of products with digital elements. NOTES that the Cyber Resilience Act proposal has a potential to significantly contribute to the strengthening of ICT supply chain security. ENCOURAGES constructive negotiations and timely adoption of the Act.**

17. In this regard, RECOGNISES the ongoing work led by ENISA, along with Member States and other stakeholders, to provide the EU with certification schemes for ICT products, services and processes in line with Cybersecurity Act that should contribute to raising the overall level of cybersecurity within the Digital Single Market. ENCOURAGES all stakeholders to participate in the preparatory work on individual European certification schemes in order to build trust in secure ICT products, processes, and services and to strengthen their resilience and CALLS on the Commission to swiftly prepare implementing acts on the European certification schemes after the completion of preparatory work, notably the Common Criteria-based European cybersecurity certification scheme (EUCC). NOTES that the European certification schemes should include, where needed, requirements on supply chain security, including relationships with suppliers.

18. HIGHLIGHTS the need for a thorough implementation of all the forthcoming NIS 2 provisions related to ICT supply chain security. In this regard, UNDERLINES the relevance of the EU coordinated risk assessments of critical supply chains (coordinated supply chain risk assessments), national policies on ~~the~~ supply chain security and **supply chain related** security measures ~~concerning the relationship of entities and their suppliers or service providers~~. NOTES that attention should be paid not only to the primary suppliers but also to the relevant subcontractors with regards to risks to the security of the primary supplier or the end customer. In order to facilitate the implementation of supply chain risk management measures, ENCOURAGES ENISA to perform, with the assistance of the NIS Cooperation Group, a stock-taking of best practices available for supply chain risk management and compile them into methodological guidelines. In addition, ENCOURAGES ENISA to monitor investments in the ICT supply chain security **of the entities regulated under the forthcoming NIS 2 Directive**.

19. HIGHLIGHTS also the benefits and risks of using Managed Service Providers (MSPs) and Managed Security Service Providers (MSSPs) in the context of supply chain security. While using these providers can significantly improve security within organisations, and lead to higher levels of cybersecurity~~. On the other hand~~, remote management of ICT systems and services combined with privileged access to the customers' ICT environment, which MSPs and MSSPs might need, can in **the** case of ~~compromising~~ **compromised** MSPs or MSSPs lead to impactful cascading effects on a large number of customers. Therefore, it is of utmost importance that MSPs and MSSPs maintain a high level of their own internal security and the security of the services they provide and take a transparent approach to their customers regarding the security of the services their provide. In this regard, WELCOMES their future inclusion into the scope of the forthcoming NIS 2 Directive.

20. Regarding the implementation of the mechanism for coordinated supply chain risk assessments pursuant to the forthcoming NIS 2 Directive. NOTES the relevance of non-technical risk factors in this context, such as undue influence by a third State on suppliers and service providers and in this context RECOGNISES the factors that can be used to assess the risk profile as mentioned in the EU coordinated risk assessment of the cybersecurity of 5G networks. INVITES the Commission to identify by the second quarter of 2023, after consulting the NIS Cooperation Group and ENISA, the specific ICT services, systems or products that might be subjected to the coordinated supply chain risk assessments with priority.

21. NOTES that dependencies on high-risk suppliers of ICT products and services used for the operation of critical networks and systems pose a strategic threat that needs to be mitigated through appropriate policies at both national and EU level and through cooperation among Member States and with like-minded international partners. In order to facilitate the mitigation of this strategic risk and support the coordinated supply chain risk assessments, INVITES the NIS Cooperation Group, in cooperation with the Commission and ENISA, to develop a toolbox of ~~identification and mitigation~~ measures for **reducing** critical ICT supply chain risks (ICT Supply Chain Toolbox). The ICT Supply Chain Toolbox should build upon strategic threat scenarios identified for ICT supply chains and provide ~~generic risk identification and mitigation strategies~~ **measures** for **responding to** these scenarios leveraging experiences from the 5G Toolbox and those gained at national level. It should complement, in a transparent way, the coordinated supply chain risk assessments for specific ICT services, systems, or products under the forthcoming NIS 2 Directive by offering generic **measures for reducing risks** ~~mitigation strategies~~ that can be adjusted for specific ICT services, systems, or products in a scalable way, on the basis of the risks identified in the individual coordinated supply chain risk assessments.

22. STRESSES the important role of research, innovation, investments and entrepreneurial activities in the digital and cybersecurity area as well as of the funding of such activities as concerns avoiding possible future unwanted strategic dependencies and strengthening the overall resilience of the ICT supply chains. In this context, EMPHASISES the role and relevance of both the strategic and implementation tasks of the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (ECCC) for contributing to maximising the effects of investments to strengthen the Union's leadership and open strategic autonomy in the area of cybersecurity and Union's support technological capacities and skills and to increase the Union's global competitiveness. In this regard, CALLS for the speedy operationalisation of the ECCC. INVITES the ECCC to take into account the ICT supply chain security aspects, including, for instance, secure software development, into their Strategic Agenda while ensuring consistency and complementarity and avoiding any duplication of effort. SUPPORTS enhancing European competitiveness in the field of cybersecurity through funding programmes, such as the Horizon Europe Programme for research and innovation as well as the Digital Europe Programme for reinforcing, building and acquiring essential capacities to EU digital economy, society and democracy.

SUPPORTING MECHANISMS

23. ENCOURAGES boosting financial support incentives related to measures aimed at strengthening ICT supply chain security. CALLS ON, as a matter of priority, also in view to the upcoming implementation of the NIS 2 Directive, the ECCC, the Commission and relevant stakeholders to ~~include dedicated Union financial support for~~ **explore options for including** ICT supply chain security aspects in the upcoming calls within the Cybersecurity Work Programmes under the Digital Europe Programme and Horizon Europe Programme, or any other relevant funding opportunities. These funding opportunities should, amongst others, be aimed at allowing the organizations to support maintaining a high level of cybersecurity in terms of the procurement of ICT products and services throughout the supply chain, particularly in relation to the replacement of specific critical ICT services, systems or products acknowledged as high-risk in accordance with the future coordinated supply chain risk assessments.

24. ACKNOWLEDGES that globalisation and the specialisation of ICT services and increased dependence on third-party products and services brings the need for close cooperation within the EU and internationally in sharing knowledge and expertise among relevant stakeholders and ENCOURAGES them to find a strong and coordinated position ensuring the security of the ICT supply chain in a comprehensive manner. ACKNOWLEDGES also the need to further explore relevant state-of-the-art approaches and techniques, both for appropriate basic cyber hygiene and long-term solutions for achieving secure and resilient ICT supply chains as well as the most suitable ways of their promotion and potential incorporation into policy or other initiatives. RECOGNISES in that regard that special attention should be given to exploring the benefits and drawbacks of systematic solutions, such as the zero-trust ~~security model~~ **principles**, software bill of materials, and similar long-term solutions. RECOMMENDS using the NIS Cooperation Group for that purpose.

25. NOTES the benefits of monitoring and effective sharing of information on cyber incidents and threats for the prevention, detection, and mitigation of effects of supply chain attacks. EMPHASISES the need to ~~building of~~ **continue building** trust and confidence between Member States for effective sharing of such information. RECALLS in that regard the Commission's proposal to support Member States in establishing and strengthening Security Operation Centres (SOCs) in order to build a network of SOCs across the EU, to further monitor and anticipate signals of attacks on networks. REMINDS the need for complementarity and coordination within existing networks and mechanisms, most notably HIGHLIGHTS in this regard the role of the CSIRTs Network and the need for further exploring these networks potential to promote an efficient, secure, and reliable information-sharing culture. RECALLS the efforts undertaken by Member States, supported by the EU, to set up sectoral, national, and regional CSIRTs and national or European Information Sharing and Analysis Centres (ISACs) as part of an effective network of cybersecurity partnerships in the Union.

26. Due to the interconnected and global nature of ICT supply chain threats, HIGHLIGHTS the importance of approaching and enhancing ICT supply chain security at the global level. In view of this, RECOMMENDS using digital partnerships, ~~free-trade agreements,~~ cyber dialogues and other relevant EU initiatives, **including, where appropriate, free-trade agreements,** for the promotion of risk-based evaluations of ICT product suppliers and ICT services providers, the use of trustworthy suppliers and for the employment of **a** secure and innovative digital ecosystem based on open, interoperable and transparent standards. In addition, REITERATES the vision of the Global Gateway partnerships as well as the EU-US Trade and Technology Council, and activities under its working groups, to promote the use of trusted/non-high-risk suppliers and to develop a financing mechanism for enabling projects making ICT infrastructure and services in third States more secure, resilient and trusted, including by refraining from financing purchases from untrusted/high-risk suppliers in a technology-neutral manner.

27. REAFFIRMS its commitment to contribute to and promote an open, free, global, stable and secure cyberspace and to adhere to the norms, rules and principles of responsible state behaviour in cyberspace laid out in the UN framework. In relation to ICT supply chain security in particular, RECALLS the norm endorsed by the UN GGE and the OEWG encouraging States to take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products, and seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, and ADVOCATES for its broad implementation.