Council of the European Union

Brussels, 14 July 2022
(OR. en)

11237/22

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 draft Council conclusions on ICT supply chain security. The draft will be submitted for discussion to the Horizontal Working Party on Cyber Issues.

ANNEX

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 geopolitical considerations for ensuring cybersecurity, EMPHASIZES that the European Union and its Member States need to approach cybersecurity in a comprehensive and strategic manner. Russia's war of 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 compromised and misused for both actions based on geopolitical rivalry, as illustrated by the SolarWinds attack, and affected by geopolitical tensions and instability, as shown by the threat caused by the reliance on Russian vendors at the time of Russia's military aggression against Ukraine.

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

2. 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 avoid similar situations of major strategic external dependencies in relation to ICT products and services. Specifically in relation to potential strategic dependencies related to ICT products and services, NOTES that the character of the risks associated with these products and services brings unique challenges and potentially far-reaching consequences. Besides the risks related to the unavailability of ICT products occurring, 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 integrity, confidentiality and availability of transmitted and stored sensitive data. Because of this and the growing digitalization of society and the ever-increasing use of ICTs in critical infrastructure, strategic external dependencies related to ICT products and services should be continuously assessed and addressed.

3. 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, and through the future Regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act) also in relation to all kinds of semiconductors which are the basic building blocks for ICT products and services. 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.

4. 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 the need to ensure the availability and diversity of ICT products and services in the Single Market while maintaining a high level of their security. ACKNOWLEDGES the need to maximize 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 to prevent potential supply chain attacks and disruptions and to mitigate their impact, notably in relation to emerging and disruptive technologies.

5. 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 continually monitor, analyze, and assess the supply chain threat landscape to raise awareness and build knowledge in order to adjust to new threats and WELCOMES the work of ENISA related to ICT supply chain security, particularly its Report on the Threat Landscape for Supply Chain Attacks. ENCOURAGES ENISA to further focus on cyber threats and challenges related to ICT supply chains, including on monitoring of investments in ICT supply chain security and assessing the implications of the use of open-source software for software supply chain security.

6. Recognising an all-hazard approach is needed in securing ICT assets, 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, , economic threats, or human errors, which may also negatively affect the supply chains of ICT products and services in the Union, particularly those which are essential for the functioning of the Single Market. Taking into account the variety of threat factors, RECOGNISES that ICT supply chain security encompasses the protection of data or ICT systems and services, delivered within the ICT supply chains, from any events that have negative effects on their confidentiality, integrity or availability.

UNIVERSAL INSTRUMENTS AND APPROACHES

7. 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 a major dependency on a single supplier, and in particular a high-risk supplier, as it increases the exposure to the consequences of potential disruptions, especially from third States. 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 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 harmonized rules on fair access to an 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.

8. RECOGNISES the link of ICT supply chain security to public procurement. EMPHASISES that the current regulation on public procurement does not adequately take into account the importance of ICT supply chain security and does not provide a sufficient range of means for the exclusion of tenderers who, for some relevant reasons not based on current criteria for qualitative selection, 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 2024 and to assess and, where needed, make proposals to revise relevant provisions in order to encourage the contracting authorities to put appropriate focus on the cybersecurity practices of tenderers and their subcontractors.

9. ACKNOWLEDGES that foreign direct investments related to ICT products and services 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. Information exchanged and shared through this mechanism can 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 duly account for this dimension of the screening mechanism.

10. With regards to the defence sector, 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.

CYBER-SPECIFIC INSTRUMENTS

11. 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 5G Toolbox emphasizing the threat of interference caused by third States through the 5G supply chain. CALLS on Member States to further exchange information on best practices and methodologies regarding the implementation of relevant key 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 RECOGNIZES it to be a valuable instrument to further enhance, in full transparency, the supply chain security of 5G networks that might serve as an inspiration for risk assessment tools related to other vital sectors. RECALLS the invitation of relevant stakeholders to formulate recommendations, based on risk assessments, to Member States and the Commission in order to reinforce the communications networks and infrastructures' resiliency within the European Union, including by implementing the EU 5G Toolbox.

12. HIGHLIGHTS the relevance of existing and forthcoming cybersecurity horizontal legislative instruments, notably the Cybersecurity Act, the forthcoming Directive on measures to achieve a high common level of cybersecurity across the Union (NIS2) and the future 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 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 networks and systems of assessing the compliance of suppliers with those obligations, while taking into account sector specificities.

13. [CRA placeholder: *WELCOMES the effort to advance the secure development of ICT products and ancillary services in the Cyber Resilience proposal….*]

14. 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 that should contribute to raising the overall level of cybersecurity within the Digital Single Market. ENCOURAGES all stakeholders' involvement 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. In order to contribute to limiting the cyber attack surface and vulnerabilities arising from ICT supply chain, the European certification schemes should encompass the security by default and by design approach, as well as include requirements aimed at, inter alia, identifying and documenting known dependencies and vulnerabilities, and ensure that authorised persons, programs or machines are able only to access the data, services or functions to which their access rights refer.

15. HIGHLIGHTS the need for a thorough implementation of all the forthcoming NIS 2 provisions related to ICT supply chain security, notably those on the EU coordinated risk assessments of critical supply chains, national policies on the supply chain security and security measures encompassing security-related aspects concerning the relationship of entities and their suppliers or service providers. NOTES that focus should be put not only on the primary suppliers but also on 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 a stock-taking of best practices available for supply chain risk management and compile them into methodological guidelines for the voluntary use of national authorities and regulated entities.

16. 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 organizations, remote management of ICT systems and services combined with privileged access to the customers' ICT environment, which MSPs and MSSPs might need, can in case of compromising 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 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.

17. Regarding the implementation of the mechanism for coordinated supply chain risk assessments pursuant to the forthcoming NIS 2 Directive, EMPHASISES the relevance of non-technical risk factors in this context, such as undue influence by a third State on suppliers and service providers, and INVITES the Commission to identify by Q2 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.

18. 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 Union level and through cooperation among Member States and between Member States partners. In order to facilitate the mitigation of this strategic threat 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 mitigation measures for 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 mitigation strategies for 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 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.

19. 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 strategic dependencies and strengthening the overall resilience of the ICT supply chains. In this context, EMPHASIZES 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 field of cybersecurity and support technological capacities and skills and to increase the Union's global competitiveness. INVITES the relevant actors within the ECCC to take into account the focus on the ICT supply chain security aspects, including, for instance, secure software development, into their Strategic Agenda while ensuring consistency and complementarity and while 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 capacity-building measures.

SUPPORTING MECHANISMS

20. 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 Commission, after consulting with the Member States, to include dedicated Union financial support for 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 be specifically 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.

21. ACKNOWLEDGES that globalization and the specialization of ICT services and increased dependence on third-party products and services brings the need for close cooperation within the EU in sharing knowledge and expertise among relevant stakeholders and ENCOURAGES them to find a strong and unified 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, software bill of materials, and similar solutions aiming at limiting the attack surface. RECOMMENDS using the NIS Cooperation Group for that purpose.

22. 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. 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 the CSIRTs Network, when 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.

23. 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, cyber dialogues and other relevant Union initiatives 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 digital ecosystem that is secure, innovative and based on open, interoperable and transparent standards. In addition, REITERATES the vision of 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.

24. 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. In relation to ICT supply chain security in particular, RECALLS the norm articulated by the UN GGE and endorsed by 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.