European Parliament
2019-2024

TEXTS ADOPTED

P9_TA(2021)0286

The EU's Cybersecurity Strategy for the Digital Decade

European Parliament resolution of 10 June 2021 on the EU's Cybersecurity Strategy for the Digital Decade (2021/2568(RSP))

The European Parliament,

– having regard to the joint communication from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 16 December 2020 entitled 'The EU's Cybersecurity Strategy for the Digital Decade' (JOIN(2020)0018),

– having regard to the Commission proposal of 16 December 2020 for a directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 (COM(2020)0823),

– having regard to the Commission proposal of 24 September 2020 for a regulation of the European Parliament and of the Council on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014 and (EU) No 909/2014 (COM(2020)0595),

– having regard to the Commission proposal of 12 September 2018 for a regulation of the European Parliament and of the Council on establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres (COM(2018)0630),

– having regard to the Commission communication of 19 February 2020 entitled 'Shaping Europe's Digital Future' (COM(2020)0067),

– having regard to Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)[1],

– having regard to Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC[2],

---

1 OJ L 151, 7.6.2019, p. 15.
2 OJ L 153, 22.5.2014, p. 62.

– having regard to Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code[1],

– having regard to Regulation (EU) No 1290/2013 of the European Parliament and of the Council of 11 December 2013 laying down the rules for participation and dissemination in 'Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020)' and repealing Regulation (EC) No 1906/2006[2],

– having regard to Regulation (EU) No 1291/2013 of the European Parliament and of the Council of 11 December 2013 establishing Horizon 2020 – the Framework Programme for Research and Innovation (2014-2020) and repealing Decision No 1982/2006/EC[3],

– having regard to Regulation (EU) 2021/694 of the European Parliament and of the Council of 29 April 2021 establishing the Digital Europe Programme and repealing Decision (EU) 2015/2240[4],

– having regard to Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport[5],

– having regard to the Budapest convention on cybercrime of 23 November 2001 (ETS No. 185),

– having regard to its resolution of 16 December 2020 on a new strategy for European SMEs[6],

– having regard to its resolution of 25 March 2021 on a European strategy for data[7],

– having regard to its resolution of 20 May 2021 on shaping the digital future of Europe: removing barriers to the functioning of the digital single market and improving the use of AI for European consumers[8],

– having regard to its resolution of 21 January 2021 on closing the digital gender gap: women's participation in the digital economy[9],

– having regard to its resolution of 12 March 2019 on security threats connected with the rising Chinese technological presence in the EU and possible action on the EU level to reduce them[10],

---

1 OJ L 321, 17.12.2018, p. 36.
2 OJ L 347, 20.12.2013, p. 81.
3 OJ L 347, 20.12.2013, p. 104.
4 OJ L 166, 11.5.2021, p. 1.
5 OJ L 207, 6.8.2010, p. 1.
6 Texts adopted, P9_TA(2020)0359.
7 Texts adopted, P9_TA(2021)0098.
8 Texts adopted, P9_TA(2021)0261.
9 Texts adopted, P9_TA(2021)0026.
10 OJ C 23, 21.1.2021, p. 2.

– having regard to the question to the Commission on the EU's Cybersecurity Strategy for the Digital Decade (O-000037/2021 – B9-0024/2021),

– having regard to Rules 136(5) and 132(2) of its Rules of Procedure,

A. whereas the digital transformation is a key strategic priority of the Union that inevitably is associated with more exposure to cyber threats;

B. whereas connected devices, including machines, sensors, industrial components and networks that make up the Internet of Things (IoT), continue to increase in number, with 22.3 billion devices expected to be linked to the IoT worldwide by 2024, thereby increasing the exposure to cyber-attacks;

C. whereas technological progress – such as quantum computing – and asymmetries in access thereto could represent a challenge for the cybersecurity landscape;

D. whereas the COVID-19 crisis has further exposed cyber-vulnerabilities in some critical sectors, particularly in healthcare, and the associated measures of teleworking and social distancing have increased our dependency on digital technologies and connectivity, while cyber-attacks and cyber-crime, including espionage and sabotage, as well as the entering and manipulation of ICT systems, structures and networks by means of malicious and unlawful installation, are increasing in number and sophistication across Europe;

E. whereas the number of cyber-attacks is increasing significantly, as seen in the recent series of malicious and organised cyber-attacks on healthcare systems such as in Ireland, Finland and France; whereas these cyber-attacks cause significant damage to healthcare systems and patient care, as well as to other sensitive public and private institutions;

F. whereas hybrid threats are increasing, including the use of disinformation campaigns and cyber-attacks on infrastructure, economic processes and democratic institutions, and are becoming a serious issue in both the cyber- and physical world, and risk affecting democratic processes such as elections, legislative procedures, law enforcement and justice;

G. whereas there is an increasing reliance on the core function of the internet and essential internet services for communication and hosting, applications and data, for which the market share is progressively being concentrated in ever fewer companies;

H. whereas distributed denial-of-service attack capabilities are growing and, therefore, the resilience of the core of the internet should be increased in parallel;

I. whereas cyber-security readiness and awareness among businesses, in particular SMEs and individuals, remain low and there is a shortage of skilled workers (the workforce gap has widened by 20 % since 2015), with traditional recruitment channels not meeting demand, including for managerial and interdisciplinary positions; whereas 'nearly 90 % of the global cybersecurity workforce is male' and 'the persistent lack of gender diversity restricts the talent pool further'[1];

---

1 European Court of Auditors *Challenges to effective EU cybersecurity policy*, briefing paper, March 2019.

J. whereas cyber-security capabilities are heterogeneous among the Member States and incident reporting and information sharing among them is neither systematic nor comprehensive, while the use of Information Sharing and Analysis Centres (ISACs) for the exchange of information between the public and private sectors is not realising its potential;

K. whereas there is a lack of agreement at EU level on cyber-intelligence collaboration and the collective response to cyber- and hybrid attacks; whereas countermeasures against cyber-threats and cyber-attacks, especially those of a hybrid nature, are technically and geopolitically very difficult for Member States to tackle alone;

L. whereas cross-border data sharing and global data sharing are important for value creation provided that privacy and intellectual and property rights are ensured; whereas the enforcement of foreign data laws could pose a cyber-security risk to European data given that companies operating in different regions are subject to overlapping obligations regardless of the location of the data or their origin;

M. whereas cyber-security represents a global market of EUR 600 billion, with this amount expected to increase rapidly, and the Union is a net importer of products and solutions;

N. whereas there is a risk of fragmentation of the single market due to national regulations on cyber-security and the lack of horizontal legislation regarding essential cyber-security requirements for hardware and software, including connected products and applications;

1. Welcomes the initiatives outlined by the Commission in the joint communication entitled ‘The EU’s Cybersecurity Strategy for the Digital Decade’;

2. Calls for the promotion of the development of secure and reliable network and information systems, infrastructure and connectivity across the Union;

3. Calls for the goal to be set that all internet-connected products in the Union, including for consumer and industrial use, along with the whole of the supply chains which make them available, need to be secure-by-design, resilient to cyber-incidents and quickly patched when vulnerabilities are discovered; welcomes the Commission’s plans to propose horizontal legislation on cyber-security requirements for connected products and associated services, and requests that such legislation propose the harmonisation of national laws to avoid fragmentation of the single market; requests that existing legislation (the Cybersecurity Act, the New Legislative Framework, the Regulation on Standardisation) be taken into account to avoid ambiguity and fragmentation;

4. Calls on the Commission to assess the need for a proposal on a horizontal regulation introducing cyber-security requirements for applications, software, embedded software and operating systems by 2023, building upon the EU *acquis* for risk management requirements; stresses that outdated applications, software, embedded software and operating systems (i.e. no longer receiving regular patches and security updates) represent a non-negligible share of all connected devices and a cyber-security risk; calls on the Commission to include this aspect in its proposal; suggests that the proposal should include obligations for producers to communicate in advance the minimum period during which they will support security patches and updates to enable buyers to make informed choices; considers that producers must be part of the Coordinated Vulnerability Disclosure (CVD) programme as set out in the proposal for the NIS2 Directive;

5. Underlines that cyber-security should be embedded in digitalisation; calls, therefore, for digitalisation projects financed by the Union to include cyber-security requirements; welcomes the support for research and innovation in the field of cyber-security, especially as regards disruptive technologies (such as quantum computing and quantum cryptography), the emergence of which could destabilise the international balance; calls, moreover, for further research on post-quantum algorithms as a cyber-security standard;

6. Considers that digitalisation of our society means that all sectors are interconnected and the weaknesses in one sector can hamper others; insists, therefore, that cyber-security policies be incorporated into the EU digital strategy and EU funding, and that they be coherent and interoperable across sectors;

7. Calls for a coherent use of EU funds as regards cyber-security and related infrastructure deployment; calls on the Commission and the Member States to ensure that cyber-security-related synergies between different programmes are exploited, in particular the Horizon Europe programme, the Digital Europe programme, the EU Space Programme, the EU Recovery and Resilience Facility, InvestEU and the CEF, and to make full use of the Cybersecurity Competence Centre and Network;

8. Recalls that communication infrastructure is the cornerstone of all digital activity and that ensuring its security is a strategic priority for the Union; supports the current development of the EU's cyber-security certification scheme for 5G networks; welcomes the EU toolbox on 5G cyber-security and invites the Commission, the Member States and industry to continue their efforts towards secure communication networks, including measures regarding the whole supply chain; calls on the Commission to avoid vendor lock-in and to enhance network security by promoting initiatives that enhance virtualisation and cloudification of the different components of the networks; calls for the quick development of the next generations of communications technologies with cyber-security-by-design as a fundamental principle and ensuring the protection of privacy and personal data;

9. Reiterates the importance of establishing a new, robust security framework for EU critical infrastructures in order to safeguard EU security interests and build on existing capabilities to respond appropriately to risks, threats and technology change;

10. Calls on the Commission to prepare provisions to ensure the accessibility, availability and integrity of the public core of the internet and, therefore, the stability of cyber-space, particularly as regards the EU's access to the global DNS root system; considers that such provisions should include measures for the diversification of suppliers to mitigate the current risk of reliance on the few companies that dominate the market; welcomes the proposal for a European Domain Name System (DNS4EU) as a tool for a more resilient internet core; asks the Commission to evaluate how this DNS4EU could use the latest technologies, security protocols and cyber-threats expertise in order to offer a fast, secure and resilient DNS for all Europeans; recalls the necessity of better protection of the Border Gateway Protocol (BGP) in order to prevent BGP hijacks; recalls its support for a multi-stakeholder model for internet governance, of which cyber-security should represent one of the core topics; underlines that the EU should speed up implementation of IPv6.; recognises the open source model which, as the basis for the internet's functioning, has proven efficient and effective; encourages, therefore, its use;

11. Recognises the need to increase cyber-security forensics to combat crime, cyber-crime and cyber-attacks, including state-sponsored attacks, but warns against disproportionate measures that jeopardise the privacy and freedom of speech of EU citizens while using the internet; recalls the need to conclude the revision of the second additional protocol to the Budapest Convention on Cybercrime, which has the potential to increase preparedness against cybercrime;

12. Calls on the Commission and the Member Stated to pool their resources to enhance the EU's strategic resilience, to reduce its dependency on foreign technologies and to propel its leadership and competitiveness in cyber-security across the digital supply chain (including data storage and processing in clouds, processor technologies, integrated circuits (chips), ultra-secure connectivity, quantum computing and the next generation of networks);

13. Considers the plan for an ultra-secure connectivity infrastructure to be an important instrument for the security of sensitive digital communications; welcomes the announcement of the development of an EU space-based global secure communications system, integrating quantum encryption technologies; recalls that continuous efforts should be made, in cooperation with the European Union Agency for the Space Programme (EUSPA) and the European Space Agency (ESA), to secure European space activities;

14. Regrets that the information sharing practices surrounding cyber-threats and incidents have not been well embraced by the private and public sectors; calls on the Commission and the Member States to increase trust and reduce barriers for sharing information on cyber-threats and cyber-attacks at all levels; welcomes the efforts made by some sectors and calls for cross-sector collaboration as vulnerabilities are rarely sector specific; highlights that Member States need to join forces at European level, in order to share efficiently their latest knowledge on cyber-security risks; encourages the formation of a Member States Working Group on Cyber-Intelligence, in order to foster the sharing of information in the EU and the European economic space, in particular, to prevent large-scale cyber-attacks;

15. Welcomes the planned establishment of a Joint Cyber Unit to strengthen cooperation between EU bodies and Member States' authorities responsible for preventing, deterring and responding to cyber-attacks; calls on the Member States and the Commission to further enhance cyber-defence cooperation and develop research in state-of-the-art cyber-defence capabilities;

16. Recalls the importance of the human factor in the cyber-security strategy; Calls for continued efforts to spread cyber-security awareness, including cyber-hygiene and cyber-literacy;

17. Highlights the importance of a robust and consistent security framework to protect all EU personnel, data, communication networks and information systems, and decision-making processes against cyber-threats based on comprehensive, consistent and homogeneous rules and adequate governance; calls for sufficient resources and capabilities to be made available, including in the context of the reinforcement of the mandate of CERT-EU and with regard to the ongoing discussions on the definition of common binding rules on cyber-security for all EU institutions, bodies and agencies;

18. Calls for the wider use of voluntary certification and cyber-security standards, as they represent important tools to improve the general level of cyber-security; welcomes the establishment of the European Certification Framework and the work of the European Cyber Security Certification Group; calls on ENISA and the Commission to consider, when preparing the EU Cybersecurity Certification Scheme for Cloud Services, making the application of EU law mandatory as regards the 'high' assurance level;

19. Highlights the need to match the cyber-security labour demand with closing the skills gap by continuing the efforts on education and training; calls for particular attention to be paid to eliminating the gender gap, which also present in this sector;

20. Recognises the need for better support for micro-, small and medium-sized enterprises to increase their understanding of all the information security risks and opportunities to improve their cyber-security; calls on ENISA and national authorities to develop self-testing portals and best practice guides for micro-, small and medium-size enterprises; recalls the importance of training and access to dedicated funding for the security of these entities;

21. Instructs its President to forward this resolution to the Commission, the Council and the governments and parliaments of the Member States.