

Draft Resolution on Cybersecurity

Submitted by Carlo Maria Palermo

Nowadays, digital dimension encompass all sphere of human life and human development. The inner implications of Information Technology make possible free access to information, services to individuals and company making possible communications among different subjects around the world.

The Information technology shaped the life of companies, define production standards, enters deeply in daily life of citizens, juridical subjects, influenced operations of private and public sector, including governmental and military operations and communications.

Aware

- That the digital sphere essential for EU and National Security, That the growing increase of multiple threats in digital sphere in daily private and public operation sphere, including different series of crimes (i.e., data theft; frauds; blackmail; fraudulent services' blockage actions; ransomware actions; cyberterrorism; attacks on supply chains),
- that disinformation and fake news, on internet media and social networks, represent a devastating phenomenon in contemporary society,
- that the Communication and operations safety concerned intimately the organization of public powers and military, intelligence operation at every level often put in danger by action of different kind of perpetrators (hackers with fraud purpose, state-backed cybercriminals, hacktivism),
- During international tensions (even during Russia-Ukraine War) digital sphere has been confrontation terrain for informatic and hybrid attacks,
- the growing threats coming from the challenge imposed by autocratic powers who proved their will to alterate the democratic process in the West (in United States and Europe) via campaign through different channels in digital sphere, mainly during sensitive electoral appointments,

Welcomes

- the *EU Cybersecurity act* as good step ahead in growing capability of the Union in order to tackle multiple threats coming from the digital sphere, together with the creation of the European Agency for Cybersecurity (ENISA),
- the supplementary funds coming from Recovery Plan on Cybersecurity a sign of commitment by the European Institutions as well as current Horizon Europe funding mechanisms

Considers

- the growing importance of digital security calls for a further step of cooperation to build a European industrial ecosystem in order to produce and support own European technology in key sector of economy and to the National security,
- Essential for European and National Security the construction of an intelligence unit devoted to cybersecurity able to enhance European cooperation and information sharing in a time when the Member States are not always prone to share vital informations,
- not be longer postponed the creation of a common consultation network in order to define threats and incidents, monitoring the cybersphere (mainly social networks) in sensitive time of elections throughout Europe,

43

44

Underlines

45

- That just the creation of a common intelligence and cybersecurity unit as part of a fully accountable foreign and security policy, as defining power of the European Federation is an essential goal to be achieved,

46

47

48

49

Asks

50

- To the Member States and EU institution to continue their action toward cybersecurity and digital security continuing their legislative effort;

51

52

53

- To enhance CSDP and NATO structures in order to build a resilient structure in order to protect vital institution of the European Union, Member States from cyberattacks,

54

55

56

- enhancing of awareness of citizens, public institutions and private sector about potential threats coming from cybercrime;

57

58

59

- Enhancing EU and Member States protection in sensitive times (i.e. election turnouts) in order to secure democratic and electoral process safeguarding Freedom of speech and prevent conditioning effort made by internal or external actors willing to alterate the natural functioning of National and European democracy.

60

61

62

63

AMENDMENT FORM

Deadline for amendments to the proposed resolutions: 12:00 (CET) 28 November 2022

Completed forms should be sent to: secretariat@federalists.eu.

Please fill out one table per amendment and one amendment form per resolution. Do not add rows or columns to the tables.

Your Name:	Michael Montag
Number of the proposed resolution that you would like to amend (e.g. 1.1.):	7

Line number(s):		
	Original text	Amended text
63 -		Support citizens enhancing their knowledge on how to protect themselves against cybersecurity
Explanatory statement (optional):	With line 56 we're requesting citizens awareness which is important, here I'd like to introduce a request on training for citizens	

Line number(s):		
	Original text	Amended text
Explanatory statement (optional):		



Line number(s):		
	Original text	Amended text
Explanatory statement (optional):		

Line number(s):		
	Original text	Amended text
Explanatory statement (optional):		

For further amendments to the same resolution, please add further tables as required.