European Parliament
2019-2024

Committee on Foreign Affairs

2020/2256(INI)

22.3.2021

DRAFT REPORT

on the state of EU cyber defence capabilities
(2020/2256(INI))

Committee on Foreign Affairs

Rapporteur: Urmas Paet

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on the state of EU cyber defence capabilities
(2020/2256(INI))

The European Parliament,

– having regard to the Treaty on European Union (TEU) and the Treaty on the Functioning of the European Union (TFEU),

– having regard to the document entitled 'Shared Vision, Common Action: A Stronger Europe – A Global Strategy for the European Union's Foreign and Security Policy', presented by the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy (VP/HR) on 28 June 2016,

– having regard to the European Council conclusions of 20 December 2013, 26 June 2015, 15 December 2016, 9 March 2017, 22 June 2017, 20 November 2017 and 15 December 2017,

– having regard to Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union,

– having regard to the Council conclusions of 19 June 2017 on a framework for a joint EU diplomatic response to malicious cyber activities ('cyber diplomacy toolbox'),

– having regard to the Joint Communication to the European Parliament and the Council entitled 'Resilience, Deterrence and Defence: Building strong cybersecurity for the EU' (JOIN(2017)0450),

– having regard to Joint Declaration on EU-NATO cooperation signed in July 2018,

– having regard to Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,

– having regard to the Council conclusions on complementary efforts to enhance resilience and counter hybrid threats of 10 December 2019,

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

– having regard to the Council conclusions of 16 June 2020 on EU External Action on Preventing and Countering Terrorism and Violent Extremism,

– having regard to the Conclusions of the Council and of the Representatives of the Governments of the Member States, meeting within the Council, on the establishment of a Civilian CSDP Compact,

– having regard to Council Decision (CFSP) 2020/1127 of 30 July 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,

– having regard to Council Decision (CFSP) 2020/1537 of 22 October 2020 amending Decision (CFSP) 2019/797 concerning restrictive measures against cyber-attacks threatening the Union or its Member States,

– having regard to the Commission's communication of 24 July 2020 on the EU Security Union Strategy (COM(2020)0605),

– having regard to the Joint Communication of the Commission and the High Representative of the Union for Foreign Affairs and Security Policy to the European Parliament and the Council "The EU's Cybersecurity Strategy for the Digital Decade" of 16 December 2020,

– having regard to the Commission's proposal 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 of 16 December 2020 (COM(2020)0823),

– having regard to the Commission's proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities of 16 December 2020 (COM(2020)0829),

– having regard to its resolution of 13 June 2018 on cyber defence[1],

– having regard to Rule 54 of its Rules of Procedure,

– having regard to the report of the Committee on Foreign Affairs (A9-0000/2021),

A. whereas the EU and its Member States must further strengthen cyber resilience and develop common and robust cyber security and defence capabilities in order to respond to lasting security challenges;

B. whereas in recent years, we have seen continuous growth in cyber operations conducted by state and non-state actors;

C. whereas conflicts can take place in all physical (land, air, sea and space) and virtual (cyber) domains, and may be amplified through elements of hybrid warfare, proxy wars, offensive and defensive use of cyber capabilities and strategic attacks to disrupt critical infrastructure;

D. whereas the European External Action Service (EEAS), the European Commission and European Defence Agency (EDA) should support Member States in stepping up their efforts to deliver cyber defence capabilities and technologies, addressing all aspects of capability development, including doctrine, leadership, organisation, personnel, training, industry, technology, infrastructure, logistics and interoperability;

E. whereas EU Cyber Defence Policy Framework updated in 2018 identified priorities,

[1] OJ C 28, 27.1.2020, p. 57.

including the development of cyber defence capabilities, as well as the protection of the Common Security and Defence Policy's (CSDP) communication and information networks;

F. whereas the increasing integration of Artificial Intelligence (AI) into defence forces' offensive cyber capabilities (cyber-physical systems, including the communication and data links between vehicles in a networked system) may lead to vulnerabilities to electronic warfare attacks such as jamming, spoofing or hacking;

G. whereas raising the level of cyber security within the EU is a necessary corollary to the success of Europe's digital ambitions;

H. whereas the Council decided for the first time on 30 July 2020 to impose restrictive measures against individuals and entities responsible for or involved in various cyber-attacks in order to better prevent, discourage, deter and respond to malicious behavior in cyberspace; whereas the legal framework for targeted restrictive measures against cyber-attacks was adopted in May 2019;

I. whereas EU-NATO cooperation has increased across multiple fields, including cyber defence;

J. whereas the 2010, 2013 and 2015 consensus reports of the UN Group of Governmental Experts (UN GGE), endorsed by the UN General Assembly, constitute a universal normative framework for cyber stability, consisting of the acknowledgment that existing international law, including the UN Charter in its entirety, applies in cyberspace, as do eleven voluntary non-binding norms of responsible state behaviour, as well as confidence-building measures and capacity-building;

The state of EU cyber defence capabilities

1. Underlines that a common cyber defence policy and a substantial cyber defence capability are core elements for the development of the European Defence Union; stresses the urgent need to strengthen EU and the Member State cyber defence capabilities;

2. Recalls that the borderless nature of cyber space and the substantial number of cyber-attacks make them a threat requiring intensified EU-NATO cooperation and a coordinated Union-level response, including common Member State support capabilities;

3. Stresses that the review of the Cyber Defence Policy Framework (CDPF) should enhance coordination between EU actors, notably the EEAS, the EU Military Staff, the European Commission, the European Defence Agency (EDA), between and with Member States, as well as with the European Parliament, in order to ensure the updated CDPF achieves the EU's cyber defence objectives;

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination; urges a cooperation strategy with the EU's Computer Emergency Response Teams (CERT-EU) to protect networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU results to ensured a

level of IT security that will allow it to receive all the necessary classified and non-classified information to carry out its responsibilities under the Treaties, including as a result of the current process to replace the 2002 Inter-Institutional Agreement on access to information in the area of security and defence;

5. Notes the 2018 CDPF's objective to setup an EU Military CERT-Network; calls on Member States to significantly increase classified information sharing, to develop a European rapid and secure network to counter cyber-attacks;

6. Recalls that the 2018 EU Capability Development Priorities (CDP) made cyber defence a key priority; welcomes the EDA's projects to improve overall EU Member States efforts in this field; takes note of the EDA's CyDRE project, which should develop an enterprise architecture for cyberspace operations, including scope, functionalities and requirements, based upon national and EU legislation;

7. Underlines that the Coordinated Annual Review on Defence (CARD) is a key tool that supports of overall coherence in Member States' defence planning, and should contribute to promoting investment in defence cyber capabilities;

8. Notes that the European Defence Fund (EDF), will also support strengthening resilience, and improve preparedness, responsiveness and cooperation in the cyber domain;

9. Welcomes the progress achieved by the Permanent Structured Cooperation (PESCO) Cyber Rapid Response Team; recalls that PESCO offers excellent ways to speed up cyber security initiatives, such as through the Cyber Threats and Incident Response Information Sharing Platform and Cyber and Information Domain Coordination Centre;

10. Emphasises that in line with the Civilian CSDP Compact, civilian CSDP must be cyber resilient and support third countries, including through Monitoring, Mentoring and Advice;

11. Welcomes the Council's June 2019 framework, which allows targeted restrictive measures to deter and respond to cyber-attacks that constitute a threat to the EU or its Member States, including cyber-attacks against third countries or international organisations; welcomes the imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox;

12. Welcomes the work led by ENISA involving the Member States and interested stakeholders to provide the EU with certification schemes for ICT products, services and processes in order to raise the overall level of cybersecurity within the digital single market; stresses the EU's pivotal pioneering role in developing standards that shape the cybersecurity landscape, contribute to fair competition within the EU and on the global stage, and react to extraterritorial measures and security risks from third countries;

Strategic vision – achieving cyber defence resilience

13. Notes that the Strategic Compass will enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into capability needs, including in cyber defence, thereby increasing the ability of the EU

and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

14. Insists that the Strategic Compass should deepen the strategic culture in the cyber domain and remove any duplication of capabilities and mandates; stresses that it is essential to overcome the current fragmentation and complexity of the overall cyber architecture within the EU;

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at the EU level; urges the VP/HR and/or the Member States to increase financial and personnel resources, in particular experts in cyberforensics; calls for further funding for CERT-EU and the creation of an EU security operations centre;

16. Recalls that cyber defence has both military and civilian dimensions; calls on the VP/HR, therefore, to develop an integrated policy approach and close cooperation between the Military CERT-Network and CERT-EU;

17. Welcomes the joint communication by the VP/HR and the Commission entitled 'The EU's Cybersecurity Strategy for the Digital Decade', which aims to enhance synergies and cooperation between civilian, defence and space cyber work; considers the strategy a milestone for strengthening the EU's and Member States' cyber resilience, thereby contributing to European strategic sovereignty;

18. Recalls that improving cyber defence capabilities also requires civilian network and information security expertise; welcomes the proposed revision of the Directive on security of network and information systems (NIS) and of current EU law, seeking to protect critical infrastructures, enhance supply chain security and the inclusion of regulated actors in the digital ecosystem;

19. Welcomes the Commission's Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological dependencies on third parties; strongly believes that the EU needs to increase its technological sovereignty and innovation, investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing;

20. Welcomes the upcoming 'Military Vision and Strategy on Cyberspace as a Domain of Operations' which will define cyberspace as a domain of operations for EU CSDP; calls for continuous assessment of the vulnerabilities of CSDP mission information infrastructures, and for the implementation of common harmonised standards in cyber defence education, training and exercises (ETE) in support of CSDP missions;

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the

parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Strengthening partnerships and enhancing the EU's role in the international context

22. Considers that EU-NATO cyber cooperation is crucial, as it enables strong formal attribution and thus the imposition of restrictive sanctions; notes that functioning deterrence would be achieved if adversaries were aware of the catalogue of possible countermeasures (based on the severity, scale, and target of the cyber-attacks);

23. Welcomes the arrangement between the CERT-EU and the NATO Computer Incident Response Capability (NCIRC), to ensure the ability to respond to threats in real time; stresses also the importance to increase cyber defence training capabilities in IT and cyber systems in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and the NATO Communications and Information (NCI) Academy;

24. Calls for further synchronisation of EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities, avoiding duplication and acknowledging their respective responsibilities;

25. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO, the United States and other strategic partners; underlines the urgent need for implementing the widely-recognised international normative framework for responsible state behaviour in cyberspace;

26. Calls on all Member States and the EU to show leadership during discussions and initiatives under the auspices of the UN to help truly promote responsible state behaviour in cyber space, building on the consensus reports of the UN GGE endorsed by the UN General Assembly; calls for UN peacekeeping missions to be reinforced with cyber defence capacities in line with the effective implementation of their mandates;

27. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the Vice-President of the Commission / High Representative of the Union for Foreign Affairs and Security Policy, the EU agencies involved in defence and cyber security, the Secretary-General of NATO, and the national parliaments of the Member States.