State of EU cyber defence capabilities

European Parliament resolution of 7 October 2021 on the state of EU cyber defence capabilities (2020/2256(INI))

(2022/C 132/09)

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 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 (1),

— 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 from the Commission and the High Representative of the Union for Foreign Affairs and Security Policy of 13 September 2017 entitled ‘Resilience, Deterrence and Defence: Building strong cybersecurity for the EU’ (JOIN(2017)0450),

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

— 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 (Cybersecurity Act) (2),

— 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 (3),

— 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 (4),

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

— 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 Council conclusions of 9 March 2021 on the EU’s Cybersecurity Strategy for the Digital Decade,

— having regard to the statement of the European Council of 25 March 2021,

— having regard to the Open-Ended Working Group (OEWG) report of 10 March 2021,

— having regard to the UN Agenda for Disarmament — ‘Securing our Common Future’,

— having regard to the UN Sustainable Development Goals, and in particular SDG 16 aiming at the promotion of peaceful and inclusive societies for sustainable development,

— having regard to European Court of Auditors Review No 09/2019 on European defence,

— having regard to its resolution of 13 June 2018 on cyber defence (5),

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

— having regard to the report of the Committee on Foreign Affairs (A9-0234/2021).

A. whereas the EU and its Member States must further develop a cyber-security strategy which sets realistic, precise and ambitious objectives and defines policies in a clear manner in both the military and the civilian domain, and also where both sectors overlap; whereas all EU institutions and EU Member States have to work more cooperatively at all levels to build that strategy, whose main objective should be to further strengthen resilience, and as a consequence, develop common, but also better, national, robust civilian and military cyber capabilities and cooperation in order to respond to lasting security challenges;

B. whereas the EU is committed to the application of existing international law in cyberspace, in particular the UN Charter which calls on states to settle international disputes by peaceful means and to refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations;

C. whereas in recent years, we have seen continuous growth in malicious cyber operations against the EU and its Member States, conducted by state and non-state actors, which have revealed vulnerabilities in networks essential to European security; whereas offensive cyber actors are growing in diversity, sophistication and number; whereas these attacks make it a matter of priority to step up defence capacity and develop European cyber capabilities; whereas damaging cyberattacks can take place at any moment and actors at both EU and national level should be encouraged to take the necessary measures to maintain effective cyber defence capabilities constantly during peacetime;

D. whereas the COVID-19 pandemic and the increase in cyber insecurity have demonstrated that international agreements are necessary; whereas cyberattacks have significantly increased during the COVID-19 pandemic and whereas the EU and its Member States have observed cyber threats and malicious cyber activities targeting essential operators, including attacks to disrupt critical infrastructure such as energy, transportation and healthcare, as well as considerable cyber-enabled foreign interference, which have blurred the line between peace and hostility; whereas the Recovery Plan for Europe envisages additional investments in cybersecurity;

E. whereas cyberspace is now recognised as a domain of operation; whereas cyber threats are capable of compromising all traditional military domains and whereas traditional domains depend on cyber space functionality and not vice versa; whereas conflicts can take place in all physical (land, air, sea and space) and virtual (cyber) domains, may be amplified through elements of hybrid warfare, such as cyber-enabled disinformation campaigns, proxy wars, offensive and defensive use of cyber capabilities and strategic attacks on digital service providers to disrupt critical infrastructure, as well as our democratic institutions, and cause considerable financial losses;

F. whereas the European External Action Service (EEAS), the Commission and the European Defence Agency (EDA) should support Member States in coordinating and 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, interoperability and resources;

G. whereas during the development of the Requirements Catalogue 2017, which is used to identify the full range of common security and defence policy (CSDP) military requirements across a number of illustrative scenarios, the need for cyber defence capabilities emerged as a high priority;

H. whereas the successful execution of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires resilient cyber-operational capabilities;

I. whereas the EU Cyber Defence Policy Framework (CDPF) updated in 2018 identified priorities such as the development of cyber defence capabilities and the protection of the CSDP’s communication and information networks;

J. whereas in her 2021 State of the Union speech, the Commission President underlined the need for an EU cyber defence policy;

K. whereas the increasing integration of artificial intelligence (AI) into defence forces’ 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;

L. whereas raising the EU’s level of cyber security and cyber defence is a necessary corollary to the success of Europe’s digital and geopolitical ambitions and would create greater resilience, keeping pace with the growing sophistication and threat of cyberattacks; whereas an EU with a strong cybersecurity culture and strong cybersecurity technology, including the capacity to identify and attribute malicious actions in a timely and effective manner and to respond adequately, would be able to protect its citizens, as well as the security of its Member States;

M. whereas international terrorist organisations have increased their expertise in and use of cyber warfare, and cyber-attackers are using state-of-the-art technology to investigate vulnerabilities in systems and devices and to engage in large- and mega-scale cyberattacks;

N. whereas the defence and space industries are facing unprecedented global competition and major technological changes with the emergence of advanced cyber technologies; whereas the European Court of Auditors has pointed to capability gaps in the area of ICT technologies, cyber warfare and AI; whereas the EU is a net importer of cyber security products and services, which increases the risk of technological dependence on and vulnerability to non-EU operators; whereas a set of common EU AI capabilities should bridge technical gaps and ensure that Member States lacking the relevant technology-industry expertise or the ability to implement AI systems in their defence ministries are not left behind;
O. whereas the Pegasus spyware scandal showed that large numbers of journalists, human rights activists, elected representatives and other EU citizens have been spied on; whereas various state actors like Russia, China and North Korea have been involved in malicious cyber activities in pursuit of political, economic and security objectives that include attacks on critical infrastructure, cyber espionage on and mass surveillance of EU citizens, aiding disinformation campaigns, distributing malware, and limiting access to the internet and the functioning of IT systems; whereas such activities disregard and violate international law, human rights and EU fundamental rights while jeopardising democracy, security, public order and the strategic autonomy of the EU, and therefore warrant a joint EU response, such as through the framework for a joint EU diplomatic response, including the use of restrictive measures envisaged for the EU cyber diplomacy toolbox;

P. whereas the Council decided for the first time on 30 July 2020 to impose restrictive measures against individuals, entities and bodies responsible for or involved in various cyberattacks in order to better prevent, discourage, deter and respond to malicious behaviour in cyberspace; whereas the legal framework for the EU cyber sanctions regime was adopted in May 2019;

Q. whereas attribution forms are a central component in cyber diplomacy and deterrence strategies;

R. whereas in recent years, EU-NATO cooperation has increased across multiple fields, including cyber security and defence, in line with the 2016 EU-NATO Joint Declaration;

S. 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 the 11 voluntary, non-binding norms of responsible state behaviour, as well as confidence-building measures and capacity building;

State of EU cyber defence capabilities

1. Underlines that a common cyber defence policy and substantial EU level cooperation on generating common, and also better, cyber defence capabilities are core elements for the development of a deepened and enhanced European Defence Union and require a complex mix of technical, strategic and operational abilities; states that cyber defence refers to actions, instruments and processes which are proportionate and in line with international law, which include both military and civilian elements, and which aim to protect, inter alia, CSDP communication and information networks, and CSDP missions and operations, and to assist Member States; stresses the urgent need to develop and strengthen both common and Member State military cyber defence capabilities;

2. Recalls that the borderless nature of cyber space, as well as the substantial number and increasing complexity of cyberattacks, require a coordinated Union-level response, including common Member State support capabilities and Member State support for measures in the EU’s cyber diplomacy toolbox, as well as intensified EU-NATO cooperation based on information sharing between cyber crisis response teams, the exchange of best practices, enhanced training, research and exercises;

3. Welcomes the CDPF as a tool to support the development of Member States’ cyber defence capabilities; stresses that the review of the CDPF should first of all highlight the existing gaps and vulnerabilities as regards EU and national military structures; stresses the need to enhance coordination between EU institutions, agencies and bodies, between and with Member States, and with the European Parliament, in order to ensure the updated CDPF achieves the EU’s cyber defence objectives;

4. Calls on the EEAS and the Commission to further develop, in cooperation with the Member States, a comprehensive set of measures and a coherent IT security policy to strengthen resilience, but also military cyber defence coordination; urges the strengthening of cooperation with the EU’s civilian Computer Emergency Response Team (CERT-EU) to protect networks used by all EU institutions, bodies and agencies, in close cooperation with CIOs in the respective entities, and of EU institutions’, bodies’ and agencies’ communication with Member States; calls for Parliament to ensure its participation in CERT-EU results to ensure 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; calls on the EEAS to ensure adequate levels of cybersecurity for its assets, premises and activities, including its headquarters, EU delegations and CSDP missions and operations;

5. Notes the 2018 CDPF’s objective to setup an EU Military CERT-Network; calls on Member States to significantly increase classified information sharing capacities in order to facilitate information sharing where needed and useful, and to develop a European rapid and secure network to detect, assess and counter cyberattacks;

6. Recalls that the 2018 EU Capability Development Priorities established in the framework of the Capability Development Plan (CDP) reflected on the need to develop full-spectrum capabilities and made cyber defence a key priority; recalls that the CDP underlined that cyber situational awareness technologies and defensive cyber technologies are essential in countering security threats; welcomes the EDA’s support for Member States in developing their capabilities to improve cyber resilience, such as the ability to detect, withstand and recover from any cyberattack; takes note of the different activities undertaken by Member States in the framework of the EDA, including the EDA’s ‘Cyber Defence Requirements Engineering’ (CyDRE) project, which should develop an enterprise architecture for cyberspace operations, including scope, functionalities and requirements, based upon national and EU legislation;

7. Calls on Member States to define a common communication standard that could be used for classified and non-classified information, in order to enhance rapid action and ensure a secure network to counter cyberattacks;

8. Welcomes the Coordinated Annual Review on Defence (CARD) — the first fully fledged defence review at EU level — which is one of the key tools that support overall coherence in Member States’ defence spending, defence planning and defence cooperation, and should contribute to promoting investment in developing cyber defence capabilities;

9. Welcomes the progress already made under the European Defence Industrial Development Programme in the form of several relevant projects on intelligence, secured communication and cyber-defence; welcomes, in particular, the call for an easily deployable and interconnected cyber toolbox for defence and the fact that the EDF will also help to strengthen resilience and improve preparedness, responsiveness and cooperation in the cyber domain, provided that such a priority is decided upon when negotiating relevant EDF work programmes; stresses that the EU’s capacity to develop cyber defence projects depends on the control of technologies, equipment, services, data and data processing and is dependent on a trusted sectoral stakeholder base, while calling for the full implementation and enforcement of the Defence Procurement Directive (**); calls on the Member States to take advantage of the EDF to jointly develop cyber defence capabilities;

10. Welcomes the increased cooperation among Member States in the domain of cyber defence and Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) and the progress achieved in the framework of the Permanent Structured Cooperation (PESCO), including through the implementation of concrete projects such as the Cyber Rapid Response Teams and Mutual Assistance in Cybersecurity project; recalls that the EDF and PESCO offer excellent means to develop cyber defence capabilities and speed up cyber security initiatives, such as through the Cyber Threats and Incident Response Information Sharing Platform and the Cyber and Information Domain Coordination Centre; calls on all Member States to ensure coherence and focus on cyber capability, developing a strategic common approach to priorities; calls for the fostering of research and innovation and the exchange of expertise in order to harness the full potential of PESCO and the EDF; welcomes the Council’s decision of 5 November 2020 allowing third countries to join individual PESCO projects in some specific cases, given that they can add value and provide technical expertise and

additional capabilities and provided that they meet an agreed set of political, substantive and legal conditions; underlines that it might be in the strategic interest of the EU on an exceptional case-by-case basis for Member States and non-Member States to participate in cyber-related PESCO projects in order to meet more ambitious commitments, on the basis of effective reciprocity;

11. Stresses that cyber defence is considered an operational task for all CSDP missions, and that cyber resilience and related capabilities must be established, tested and deployed prior to the start of CSDP planning processes; recalls that the successful execution of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber operational capabilities, as well as adequate responses to attacks against military installations, missions and operations; emphasises that in line with the Civilian CSDP Compact, civilian CSDP missions must be cyber resilient and support host countries where appropriate, including through monitoring, mentoring and advice; recommends that options be explored to foster the cyber capability-building of our partners, such as extending the mandate of EU training missions to cover aspects of cyber defence or launching civilian cyber missions;

12. Welcomes the Council’s decision of 14 May 2019 concerning restrictive measures against cyberattacks threatening the Union or its Member States, which allows for targeted restrictive measures to deter and respond to cyberattacks that constitute a threat to the EU or its Member States, including cyberattacks against third countries or international organisations; welcomes the imposition of such restrictive measures in July 2020 and October 2020 as a credible step in implementing the EU’s cyber diplomacy toolbox, including restrictive measures, and in strengthening the EU’s cyber deterrence posture; calls for further development and strict enforcement of a system of proportionate restrictive measures to contain cyberattacks, while respecting the European vision for the internet, which is one of a single, open, neutral, free, secure and unfragmented network;

13. Recalls that given the dual nature of cyber technologies, secured civilian products and services are key to the military and thus contribute to better cyber defence; welcomes therefore 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; also acknowledges the important role of ENISA in supporting research initiatives and other forms of cooperation aimed at enhancing cybersecurity; underlines the importance of investments in cyber-defence and cybersecurity capabilities with the aim of enhancing the EU’s and Member States’ resilience and strategic capacities; highlights in this regard the importance of the Digital Europe Programme and Horizon Europe, especially its ‘Civil security for society’ cluster; notes the significance of the relevant financial instruments available under the 2021-2027 multiannual financial framework (MFF), as well as the Recovery and Resilience Facility (RRF);

14. Welcomes the progress made by some Member States in establishing cyber commands within their military;

Strategic vision — achieving cyber defence resilience

15. 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 as a priority, thereby increasing the ability of the EU and Member States to detect, attribute, prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, legal and ethical framework, tools, procedures and partnerships;

16. 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 and to develop a common vision of how to achieve security and stability in cyberspace;

17. Stresses that fragmentation is accompanied by serious concerns over the lack of resources and staff at EU level, which hinders the ambition of creating the most secure digital environment, and therefore stresses the need to increase both; urges the VP/HR and/or the Member States to increase financial and cyber defence personnel resources, in particular
cyber intelligence analysts and experts in cyber forensics, and their training in the areas of decision and policy making, policy implementation, cyber incident response and investigations, including the development of cyber skills to strengthen the EU's ability to characterise and attribute cyberattacks and hence provide an adequate political, civilian and military response within a short time frame; calls for further funding for CERT-EU and the EU Intelligence and Situation Centre (INTCEN) and support for Member States in establishing and strengthening security operation centres (SOCs) in order to build a network of SOCs across the EU which could enhance civil-military cooperation so as to provide timely warnings of cybersecurity incidents;

18. Notes that streamlined EU military training and education in the cyber domain would significantly improve the level of trust among Member States, increasing standard operating procedures, establishing clearer rules, and improving enforcement; notes in this regard the important training work undertaken by the European Security and Defence College (ESDC) in the cyber defence field, and welcomes in this respect the establishment of the Cyber Education, Training, Evaluation and Exercise (ETEB) Platform, aimed at addressing cyber security and defence training among civilian and military personnel, as well as establishing the necessary harmonisation and standardisation in cyber-related training; stresses that the ESDC should benefit more from structural Union funding so as to be able to enhance its contribution to fostering EU cyber defence skills, especially given the increased need for top-level cyber experts; calls on Member States to promote partnerships with academia aimed at fostering cybersecurity R&D programmes in order to develop new common technologies, tools and skills applicable in both the civilian and the defence sectors; stresses the importance of education to raise public awareness and improve the skills of citizens so that they may defend themselves against cyberattacks;

19. Underlines the need for EU cyber defence policies to incorporate gender considerations and to be ambitious in closing the gender gap among cyber defence professionals, notably through active gender-inclusive policies and tailored training programmes for women;

20. Recalls that cyber defence has both military and civilian dimensions and thus requires stronger cooperation, synergies and coherence among instruments; stresses the need to first analyse and discuss problems of cooperation and coordination, but then also of gaps as regards human and technical resources at both national and EU level; notes that successful integration of both military and civilian resources can only be ensured through training and exercises with all relevant stakeholders; highlights in this regard NATO’s Locked Shields exercise as one of the best examples of testing and improving cyber defence capabilities, both civilian and military; calls on the VP/HR and Commission, therefore, to develop an integrated policy approach and promote synergies and close cooperation between the Military CERT-Network, CERT-EU and the CSIRT Network;

21. 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 strengthening the EU’s digital leadership and its strategic capacities;

22. Recommends the establishment of a Joint Cyber Unit to increase cooperation with a view to responding to the lack of information sharing among EU institutions, bodies and agencies, thereby guaranteeing a secure and rapid information network, and to enabling the full use of existing structures, resources and capabilities; notes the important role the Joint Cyber Unit could play in protecting the EU from grave cross-border cyberattacks, on the basis of the concept of cross-sector information-sharing: underlines the importance of coordination in order to avoid the duplication of structures and responsibilities during its development; welcomes in this regard the Commission recommendation of 23 June 2021, which provides that specific interfaces with the Joint Cyber Unit should be built to enable information sharing with the cyber defence community, notably through EEAS representation; stresses also that representatives of relevant PESCO projects should support the Joint Cyber Unit, especially in relation to situational awareness and preparedness;

23. Recalls that, given their often dual-use nature, improving cyber defence capabilities also requires civilian network and information security expertise; stresses that the proliferation of dual-use, off-the-shelf systems may present challenges in terms of systems being exploited by an increasing number of state and non-state hostile actors; calls on the Commission
and the Member States to activate several key levers, such as certification and the supervision of the responsibility of private actors; underlines that technological innovation is mainly driven by private companies, and therefore that cooperation with the private sector and civilian stakeholders, including industries and entities involved in the management of critical infrastructures, as well as SMEs, civil society, organisations and academia, is crucial and should be reinforced; takes note of the proposed revision of the Directive on Security of Network and Information Systems (NIS) and of the proposal for a directive on the resilience of critical entities, seeking to protect critical infrastructures and enhance supply chain security and the inclusion of regulated actors in the digital ecosystem; recalls that each Member State should have a dedicated policy towards cybersecurity supply chain risk management addressing, in particular, the question of trusted vendors; recalls also that the NIS Directive should respect Member States' competencies and refers to the relevant Subcommittee on Security and Defence opinions on both proposals;

24. Welcomes the launch of the Cyber Crises Liaison Organisation Network (CyCLONe) on 29 September 2020, which further improved timely information sharing and situational awareness by closing the gap between the EU’s technical and political levels; notes that an effective cyber defence capability requires a change from a ‘need-to-know’ to a ‘need-to-share’ culture of information sharing;

25. 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, the infrastructure used to ‘create’ cyberspace is mainly operated 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 boost innovation, investing in the ethical use of new technologies in security and defence such as AI and quantum computing; strongly encourages the development of an AI-focused agenda for R&D within Member States; stresses, however, that the military use of AI must respect international human rights law and international humanitarian law, and that the EU must take the lead in promoting a global AI regulatory framework rooted in democratic values and a human-in-the-loop approach;

26. Notes the important work conducted by EU SatCen and underlines that the Union must have adequate resources in the fields of space imagery and intelligence gathering; asks the agency to analyse and provide a report regarding the safety and/or vulnerability of EU and Member State satellites to space debris and cyberattack; stresses that EU SatCen should benefit from more structural Union funding to be able to maintain its contributions to the Union’s actions; stresses that cyber defence capabilities are crucial for ensuring secured and resilient information exchange with SatCen in both security from space and in space, in order to preserve and enhance the EU’s strategic autonomy as regards situational awareness; underlines the need for the EU to strive to prevent the weaponisation of space;

27. Welcomes the Council’s decision on the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre in Bucharest, which will channel cybersecurity-related funding from Horizon Europe and the Digital Europe Programme, and encourages seamless cooperation with its network of national coordination centres; stresses the importance of the centre in implementing relevant cybersecurity projects and initiatives that will help to create the new capacities essential to underpinning Union resilience and stepping up coordination between the civilian and defence cybersecurity sectors; underlines that the Cybersecurity Competence Centre must bring together the main European stakeholders, including industry, academic and research organisations and other relevant civil society associations, to enhance and spread cybersecurity expertise across the EU;

28. Underlines the importance of encryption and legal access to encrypted data; recalls that data encryption and the enhancement and widest possible use of such capabilities can make a significant contribution to the cyber security of states, societies and industry; encourages a ‘European digital sovereignty’ programme in order to foster and enhance the current capabilities in terms of cyber and encryption tools inspired by fundamental European rights and values such as privacy, freedom of expression and democracy, with the aim of enhancing European competitiveness in the cybersecurity market and boosting internal demand;
29. 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;

30. Deplores the fact that current limitations in the classified systems of the EU Military Planning and Conduct Capability (MPCC) are hampering its capabilities; calls on the EEAS, therefore, to swiftly provide the MPCC with a state-of-the-art autonomous and secure Communications and Information System (CIS) able to handle classified EU data for its CSDP missions and operations, with an adequate level of protection and resilience and a deployed Force Headquarters;

31. Calls for further integration of cybersecurity into EU crisis response mechanisms and for the existing initiatives, structures and procedures across various cyber communities to be linked with a view to enhanced mutual assistance and operational cooperation between Member States, in particular in the event of major cyberattacks, in order to increase interoperability and develop a common understanding of cyber defence; strongly emphasises the importance of further exercises, but at a higher frequency, and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) TEU) in a hypothetical grave cyberattack scenario, potentially considered an armed attack; calls for such initiatives to strengthen common understanding of the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) TEU and Article 222 TFEU, including with a specific objective of operationalising these procedures for cyberattacks on the Member States; welcomes the NATO Brussels Summit Communiqué of 14 June 2021, reaffirming NATO’s engagement in employing the full range of capabilities at all times to actively deter, defend against, and counter the full spectrum of cyber threats, including the decision to invoke Article 5 ‘on a case-by-case basis’; welcomes further discussions on the articulation between the EU cybersecurity crisis management framework and the cyber diplomacy toolbox;

32. Notes that the EU is increasingly involved in hybrid conflicts with geopolitical adversaries; underlines that these acts are of a particularly destabilising and dangerous nature as they blur the lines between war and peace, destabilise democracies and sow doubt in the minds of target populations; recalls that these attacks are by themselves often not serious enough to trigger Article 5 of the NATO Treaty or Article 42(7) TEU, though they have a cumulative strategic effect and cannot be effectively tackled through retorsions by the injured Member State; believes that the EU should therefore strive to find a solution to fill this legal vacuum by reinterpreting Article 42(7) TEU and Article 222 TFEU in such a way that would reserve the right for collective defence below the collective defence threshold and allow for collective countermeasures by EU Member States on a voluntary basis, and should work internationally with allies towards a similar solution at international level; underlines that this is the only effective means to counter the paralysis in reacting to hybrid threats and is an instrument to increase the costs for our adversaries;

33. Reiterates that common strong attribution capabilities are one of the key tools for strengthening EU and Member State capabilities and are an essential component of effective cyber defence and cyber deterrence; stresses that the improvement of information sharing as regards technical information, analysis and threat intelligence between Member States at EU level could enable collective attribution at EU level; recognises that, to a certain degree, cyber defence is more effective if it also contains some offensive means and measures, provided that their use is compliant with international law; underlines that explicit attribution of cyberattacks is a useful instrument of deterrence; invites consideration of joint public attribution of malicious cyber activities, including the option to create cyber-behaviour reports under the auspices of the EEAS for specific actors to summarise state-sponsored malicious cyber activities against Member States at EU level;

34. Considers that EU-NATO cyber cooperation is crucial, as it could enable and strengthen formal collective attribution of cyber malicious incidents and consequently the imposition of restrictive sanctions and measures; notes that functioning resilience and effective deterrence would be achieved if perpetrators are aware of the catalogue of possible countermeasures, their proportionality and appropriateness, and their compliance with international law, in particular the UN Charter (based on the severity, scale and target of the cyberattacks);

35. Welcomes the VP/HR’s proposal to encourage and facilitate the establishment of a Member States’ EU cyber intelligence working group residing within INTCEN to advance strategic intelligence cooperation on cyber threats and activities, in order to further support EU situational awareness and decision-making as regards a joint diplomatic response;
encourages further progress in the common set of proposals, particularly the ongoing interaction with the EU Hybrid Fusion Cell and NATO's Hybrid Analysis Cell in sharing situational awareness and analysis, and in tactical and operational cooperation;

**Strengthening partnerships and enhancing the EU’s role in the international context**

36. Considers that cyber defence cooperation with NATO plays an important role in preventing, deterring and responding to cyberattacks affecting Member States' collective security; calls on Member States to fully share evidence and intelligence in order to feed into the establishment of cyber sanction lists; 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);

37. Recognises that the EU and NATO should coordinate on issues where hostile actors are threatening Euro-Atlantic security interests; expresses concern about the systemic aggressive behaviour demonstrated notably by China, Russia and North Korea in cyberspace, including numerous cyberattacks against government institutions and private companies; believes that EU-NATO cooperation should focus on challenges in the cyber, hybrid, emerging and disruptive technologies (EDT), space, arms control and non-proliferation areas; urges EU-NATO cooperation ensuring resilient, affordable and secure high-speed networks complying with EU and national security standards that secure national and international information networks capable of encrypting sensitive data and communications;

38. 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 by improving cyber incident prevention, detection and response both in the EU and in NATO; stresses also the importance of increasing 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;

39. Calls for further EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities and mutually beneficial strengthening of capacities, pursuing the affiliation of relevant CSDP structures to NATO’s Federated Mission Networking, avoiding duplication and acknowledging their respective responsibilities; urges the reinforcement of the EU’s PESCO, as well as NATO’s Smart Defence, Connected Forces Initiative and Defence Investment Pledge, and the promotion of pooling and sharing, seeking to better forge synergies and efficiencies in the relationship between suppliers and end-users; welcomes the progress made in EU-NATO cooperation in the cyber defence field, notably in the exchange of concepts and doctrines, cross-participation in cyber exercises and cross-briefings, notably on the cyber dimension of crisis management; suggests the creation of a joint EU-NATO cyber threat information hub, as well as a joint task force for cyber security;

40. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO Allies, the UN and the Organization for Security and Co-operation in Europe (OSCE); encourages, in this regard, the further promotion of the OSCE confidence-building measures for cyberspace and underlines the need to develop effective international cooperation tools to support the strengthening of partners’ cyber capacity building, as well as to develop and promote confidence-building measures and inclusive cooperation with civil society and stakeholders; welcomes the importance attributed to a global, open, free, stable and secure cyber space by the EU Strategy for Cooperation in the Indo-Pacific of 19 April 2021; calls for the active development of closer ties with likeminded democracies in the Indo-Pacific region, such as the US, South Korea, Japan, India, Australia and Taiwan, in order to share knowledge and experience and exchange information on countering cyber threats; underlines also the importance of cooperation with other countries, particularly in the EU’s immediate neighbourhood, to help build their capacity to defend against cybersecurity threats; commends the Commission’s support for cybersecurity programmes in the Western Balkans and the Eastern Partnership countries; stresses the urgent need to respect international law, including the UN Charter in its entirety, and adhere to the widely recognised international normative framework for responsible state behaviour, and to contribute to the ongoing discussion on the modalities of application of international law in cyberspace within the UN context;
41. Underlines the importance of having a strong partnership in the cyber domain with the UK, which is a leading nation in terms of its cyber defence arsenal; calls on the Commission to investigate the possibility of relaunching a process aiming to conclude a formal and structured framework for cooperation in this field in the future;

42. Emphasises the need to ensure peace and stability in cyberspace; calls on all Member States and the EU to show leadership during discussions and initiatives under the auspices of the UN, including by proposing a programme of action, to take a proactive approach to the establishment of an internationally shared regulatory framework and to help truly advance accountability, adherence to emerging norms and prevention of the misuse of digital technologies and promote responsible state behaviour in cyberspace, building on the consensus reports of the UN GGE endorsed by the UN General Assembly; welcomes the recommendations of the OEWG final report, notably on the establishment of a programme of action; encourages the UN to foster dialogue among states, researchers, academics, civil society organisations, humanitarian actors and the private sector so as to ensure inclusive policymaking processes for new international provisions; calls for all existing multilateral efforts to be accelerated so that normative and regulatory frameworks are not outpaced by technological development and new methods of warfare; calls for the modernisation of arms control architecture, in order to avoid the emergence of a digital grey zone; calls for UN peacekeeping missions to be reinforced with cyber defence capacities in line with the effective implementation of their mandates;

43. Recalls its position on a ban on the development, production and use of fully autonomous weapons enabling strikes to be carried out without meaningful human intervention; calls on the VP/HR, the Member States and the European Council to adopt a common position on autonomous weapons systems that ensures meaningful human control over the critical functions of such weapons systems; demands that international negotiations be launched on a legally binding instrument that would prohibit fully autonomous weapons;

44. Underlines the importance of cooperation with national parliaments in order to exchange best practices in the area of cyber defence:

45. 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 governments and parliaments of the Member States.