European Parliament
2014-2019

Plenary sitting

A8-0189/2018

25.5.2018

REPORT

on cyber defence
(2018/2004(INI))

Committee on Foreign Affairs

Rapporteur: Urmas Paet

CONTENTS

Page

MOTION FOR A EUROPEAN PARLIAMENT RESOLUTION

on cyber defence
(2018/2004(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 the Commission’ communication of 7 June 2017 entitled ‘Reflection Paper on the Future of European Defence’ (COM(2017)0315),

– having regard to the Commission’s communication of 7 June 2017 entitled ‘Launching the European Defence Fund’ (COM(2017)0295),

– having regard to the Commission’s communication of 30 November 2016 on the European Defence Action Plan (COM(2016)0950),

– 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, the Council, the European Economic and Social Committee and the Committee of the Regions on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace of 7 February 2013 (JOIN(2013)0001),

– having regard to the Commission staff working document of 13 September 2017 entitled ‘Assessment of the EU 2013 Cybersecurity Strategy’ (SWD(2017)0295),

– having regard to the EU Cyber Defence Policy Framework of 18 November 2014,

– having regard to the Council conclusions of 10 February 2015 on cyber diplomacy,

– 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 on Resilience, Deterrence and Defence: Building strong cybersecurity for the EU (JOIN(2017)0450),

– having regard to ‘Tallinn Manual 2.0 on the International Law Applicable to Cyber

Operations'[1],

– 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 work of the Global Commission on the Stability of Cyberspace,

– having regard to the Commission's communication of 28 April 2015 entitled 'The European Agenda on Security' (COM(2015)0185),

– 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 on the Joint Framework on countering hybrid threats a European Union response (JOIN(2016)0018) of 6 April 2016,

– having regard to its resolution of 3 October 2017 on the fight against cybercrime[2],

– having regard to the Joint Declaration of the Presidents of the European Council and the European Commission and of the Secretary-General of NATO of 8 July 2016, to the common sets of proposals for the implementation of the Joint Declaration endorsed by the EU and NATO Councils on 6 December 2016 and 5 December 2017, and to the progress reports on the implementation thereof of 14 June and 5 December 2017,

– having regard to its resolution of 22 November 2012 on Cyber Security and Defence[3],

– having regard to its resolution of 22 November 2016 on the European Defence Union[4],

– having regard to the Commission's Proposal for a Regulation of the European Parliament and of the Council on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act") of 13 September 2017,

– having regard to its resolution of 13 December 2017 on the implementation of the Common Foreign and Security Policy (CFSP)[5],

– having regard to its resolution of 13 December 2017 on the implementation of the Common Security and Defence Policy (CSDP)[6],

– having regard to Rule 52 of its Rules of Procedure,

– having regard to the report of the Committee on Foreign Affairs (A8-0189/2018),

A. whereas cyber and hybrid challenges, threats and attacks constitute a major threat to the security, defence, stability and competitiveness of the EU, its Member States and its

[1] Cambridge University Press, February 2017, ISBN 9781316822524, https://doi.org/10.1017/9781316822524.
[2] Texts adopted, P8_TA(2017)0366.
[3] OJ C 419, 16.12.2015, p. 145.
[4] Texts adopted, P8_TA (2016)0435.
[5] Texts adopted, P8_TA(2017)0493.
[6] Texts adopted, P8_TA(2017)0492.

citizens; whereas cyber defence clearly incorporates both military and civilian dimensions;

B. whereas the EU and the Member States face an unprecedented threat in the form of politically motivated, state-sponsored cyber attacks as well as cyber crime and terrorism;

C. whereas cyber space is widely recognized as the fifth operational domain by the military enabling the development of cyber defence capabilities; whereas debates are held whether to recognize cyber space as the fifth domain of warfare;

D. whereas the mutual defence clause, Article 42(7) of the TEU, provides a mutual obligation of aid and assistance by all means of power in case of an armed aggression on a territory of a Member State; whereas this shall not prejudice the specific character of the security and defence policy of certain Member States; whereas the solidarity clause, Article 222 of the TFEU, complements the mutual defence clause by providing that EU countries are obliged to act jointly where an EU country is the victim of a terrorist attack or a natural or man-made disaster; whereas the solidarity clause implies the use of both civilian and military structures;

E. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in providing a platform for European cooperation, and in ensuring that these new endeavours are closely coordinated at an international level and within the transatlantic security architecture from the start, to avoid gaps and inefficiencies that mark many traditional defence efforts; whereas we need to do more than enhance our cooperation and coordination; whereas we have to ensure effective prevention by stepping up the ability of the EU to detect, defend and deter; whereas a credible cyber defence and deterrence is needed to achieve effective cyber security for the EU while ensuring that those states that are least prepared do not become easy targets of cyber attacks, and whereas a substantial cyber defence should be a necessary part of the CSDP and the development of the European Defence Union; whereas we are in a situation of permanent shortage of highly qualified cyber defence specialists; whereas close coordination on protecting armed forces against cyber attacks is a necessary part of the development of an effective CSDP;

F. whereas EU Member States are often subject to cyber attacks conducted by hostile and dangerous state and non-state actors against civilian or military targets; whereas current vulnerability is due mainly to the fragmentation of European defence strategies and capabilities, allowing foreign intelligence agencies to repeatedly exploit the security vulnerabilities of IT systems and networks essential to European security; whereas Member State governments have often failed to inform relevant stakeholders in good time to allow them to address vulnerabilities in their products and services; whereas these attacks require urgent reinforcements and the development of European offensive and defensive capacities at civilian and military levels in order to avoid the possible cross-border economic and societal impact of cyber incidents;

G. whereas the lines between civil and military interference become blurry in cyber space;

H. whereas many cyber incidents are made possible by the lack of resilience and robustness of private and public network infrastructure, by poorly protected or secured

databases and by other flaws in the critical information infrastructure; whereas only few Member States take responsibility for the protection of their respective network and information systems, and the associated data, as part of their respective duty of care, which explains the overall lack of investment in training and state-of-the art security technology, and of the development of appropriate guidelines;

I. whereas the rights to privacy and data protection are laid down in the EU Charter of Fundamental Rights and in Article 16 of the TFEU, and are regulated by the EU's General Data Protection Regulation, which entered into force on 25 May 2018;

J. whereas an active and efficient cyber policy is one that is capable of deterring enemies as well as of disrupting their capabilities and pre-empting and degrading their ability to attack;

K. whereas several terrorist groups and organisations use cyber space as a low-cost tool for recruitment, radicalisation and the dissemination of terrorist propaganda; whereas terrorist groups, non-state actors and transnational criminal networks use cyber operations to raise funds anonymously, gather intelligence and develop cyber arms to wage cyber terror campaigns, to disrupt, damage or destroy critical infrastructure, to attack financial systems and to pursue other illegal activities that have implications for the security of the European citizens;

L. whereas the cyber deterrence and defence of Europe’s armed forces and critical infrastructure have become crucial issues in debates about defence modernisation, Europe’s common defence efforts, the future development of armed forces and their operations, and the strategic autonomy of the European Union;

M. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges and improve their cyber resilience, but much more needs to be done as it is becoming more and more difficult to counter cyber attacks at Member State level; whereas the cyber commands of the respective Member States vary in their offensive and defensive mandates; whereas other cyber defence structures vary broadly among the Member States and often remain fragmented; whereas cyber defence and deterrence are activities that can best be tackled cooperatively at European level and in cooperation with our partners and allies, as its operational domain recognises neither national nor organisational boundaries; whereas military and civilian cyber security is closely related, and more synergy between civilian and military specialists is therefore needed; whereas private companies have substantial expertise in this field, raising fundamental questions about governance and security, and about the ability of states to defend their citizens;

N. whereas there is an urgent need to strengthen the EU’s capabilities in the field of cyber defence, given the lack of a timely response to the changing cyber security landscape; whereas rapid response and adequate preparedness are key elements in ensuring security in this area;

O. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to foster an ecosystem that can provide opportunities for SMEs and start-up companies, and to facilitate cooperative projects in the cyber defence domain, and both will contribute to shape the regulatory

and institutional framework;

P. whereas Member States participating in PESCO have committed themselves to ensuring that cooperation efforts on cyber defence – such as information sharing, training and operational support – will continue to grow;

Q. whereas among the seventeen projects selected for PESCO, two projects are in the field of cyber defence;

R. whereas the EDF needs to support the global competitiveness and innovativeness of the European defence industry, by investing in digital and cyber technologies, as well as to facilitate the development of smart solutions by providing opportunities for SMEs and start-up companies to participate in this effort;

S. whereas the EDA has launched a number of projects to meet Member States' need to develop their cyber defence capabilities, including projects on education and training such as the Cyber Defence Training & Exercises Coordination Platform (CD TEXP), Demand Pooling for Cyber Defence Training and Exercise support by the private sector (DePoCyTE) and the Cyber Ranges project;

T. whereas there are other ongoing EU projects on situational awareness, malware detection and information sharing (the Malware Information Sharing Platform (MISP) and the Multi-Agent System For Advanced persistent threat Detection (MASFAD));

U. whereas capacity-building and training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at EU and NATO levels;

V. whereas CSDP missions and operations, like all modern organisational endeavours, are deeply reliant on functioning IT systems; whereas cyber threats to CSDP missions and operations can exist at different layers, ranging from the tactical layer (CSDP missions and operations) and operational layer (EU networks) to the broader layer of global IT infrastructure;

W. whereas command and control systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors seeking to attack missions; whereas cyber attacks may have serious repercussions for EU infrastructure; whereas cyber attacks against, in particular, the EU's energy infrastructure would have serious repercussions, and must therefore be guarded against;

X. whereas it is well understood that cyber defence should be duly considered at all stages of the planning process for CSDP missions and operations, that it requires constant monitoring, and that adequate capabilities need to be available to mainstream it fully into mission planning and to continuously provide the necessary critical support;

Y. whereas the European Security and Defence College (ESDC) network is the only European training provider for the CSDP structures, missions and operations; whereas, according to current plans, its role in pooling European training capacities in the cyber domain is to be increased substantially;

Z. whereas the Declaration of NATO's 2016 Warsaw Summit recognised cyber space as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea;

AA. whereas the EU and NATO have contributed to improving Member States cyber defence capabilities through dual-use research projects coordinated by the EDA and NATO, and by improving Member States cyber resilience through support provided by the European Union Agency for Network and Information Security (ENISA);

AB. whereas in 2014 NATO established cyber security operations as part of its collective defence, and in 2016 recognised cyber space as an operational domain together with land, air and sea; whereas EU and NATO are complementary partners in building their cyber resilience and cyber defence capabilities; whereas cyber security and defence is already one of the strongest pillars of cooperation between the two, and a critical field in which both have unique capacities; whereas in the EU-NATO Joint Declaration of 8 July 2016 the EU and NATO agreed to a broad agenda of cooperation; whereas four out of 42 proposals for closer cooperation concern cyber security and defence, with further proposals aimed at addressing hybrid threats in a broader sense; whereas this has been complemented by a further proposal regarding cyber security and defence presented on 5 December 2017;

AC. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it was unable to produce a consensus report in 2017, the 2015 and 2013 reports apply, including the recognition that existing international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability, and to promoting an open, secure, peaceful and accessible ICT environment;

AD. whereas the recently launched framework for a joint EU diplomatic response to malicious cyber activities, the EU cyber diplomacy toolbox – aimed at developing the EU's and Member States' capacities in order to influence the behaviour of potential aggressors – foresees the use of proportionate measures within the CFSP, including restrictive measures;

AE. whereas different state actors – Russia, China and North Korea among others, but also non-state actors (including organised crime groups) inspired, hired or sponsored by states, security agencies or private companies – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber espionage and mass surveillance of EU citizens, aiding disinformation campaigns and distributing malware (Wannacry and NotPetya, etc.) 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 should therefore lead to a joint EU response, such as using the framework for a joint EU diplomatic response, including the use of restrictive measures envisaged for the EU cyber diplomacy toolbox, such as, in the case of private companies, fines and restricted access to the internal market;

AF. whereas such large scale attacks against ICT infrastructure have been made several times in the past, including in Estonia in 2007, in Georgia in 2008 and, currently almost

on a daily basis, in Ukraine; whereas offensive cyber capabilities are also being employed against EU and NATO Member States at an unprecedented scale;

AG. whereas cyber security technologies, relevant to both the military and the civilian domain, are "dual-use" technologies that offer many opportunities for developing synergies between civilian and military actors in a number of areas, such as encryption, security and vulnerability management tools, intrusion detection and prevention systems;

AH. whereas the development of cyber technologies will in the coming years affect new fields such as artificial intelligence, the internet of things, robotics and mobile devices, and all these elements may also have security implications for the defence domain;

AI. whereas the cyber commands established by several Member States can make a substantial contribution to the protection of vital civilian infrastructure, and whereas cyber defence-related knowledge is often equally useful in the civilian domain;

Capability development for cyber defence and deterrence

1. Underlines that a common cyber defence policy, and a substantial cyber defence capability, should constitute core elements in the development of the European Defence Union;

2. Welcomes the initiative of the Commission for a cyber-security package to foster EU cyber resilience, deterrence and defence;

3. Recalls that cyber defence has both military and civilian dimensions, and that this means that an integrated policy approach, and close cooperation between military and civilian stakeholders, is required;

4. Calls for a coherent development of cyber capacities across all EU institutions and bodies, as well as in the Member States, and for providing needed political and practical solutions to overcoming the remaining political, legislative and organisational obstacles to cooperation on cyber defence; regards regular and enhanced exchange and cooperation between relevant public stakeholders in cyber defence, at EU and national level, as crucial;

5. Strongly emphasises that, in the framework of the emerging European Defence Union, the cyber defence capabilities of Member States should be at the forefront and, as far as it is possible, integrated from start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber defence, using a clear roadmap, thereby feeding into a process coordinated by the Commission, the European External Action Service (EEAS) and the EDA with a view to better streamlining cyber defence structures across the Member States, implementing available short-term measures urgently and fostering the exchange of expertise; is of the opinion that we should develop an European secure network for critical information and infrastructure; recognises that strong attribution capabilities are an essential component of effective cyber defence and cyber deterrence, and that effective prevention would require the development of substantial further technological expertise; urges the Members States to increase financial and personnel resources, in particular experts in

cyber forensics, in order to improve the attribution of cyber attacks; underlines that such cooperation should also be implemented through the enhancement of ENISA;

6. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that owing to the borderless nature of cyber space, the scale and knowledge required for truly comprehensive and effective forces ensuring the goal of strategic autonomy of the EU in cyber space is beyond the reach of any single Member State, requiring, therefore, an intensified and coordinated response on the part of all Member States at EU level; notes, against this background, that the EU and its Member States find themselves under time pressure regarding the development of such forces, and need to act immediately; notes that due to EU initiatives such as the digital single market, the EU is well placed to take a leading role in developing European cyber defence strategies; reiterates that development of cyber defence at EU level must enhance the EU's capability to protect itself; welcomes, in this regard, the proposed permanent mandate of, and strengthened role for, ENISA;

7. Urges the Member States, in this context, to make the best possible use of the framework provided by PESCO and the EDF to propose cooperation projects;

8. Takes note of the hard work done by the EU and its Member States in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

9. Welcomes the two cyber projects to be launched in the framework of PESCO, namely the Cyber Threats and Incident Response Information Sharing Platform and the Cyber Rapid Response Teams and Mutual Assistance in Cyber Security; stresses that these two projects focus on a defensive cyber policy that builds on the sharing of cyber threat information through a networked Member State platform and the establishment of Cyber Rapid Response Teams (CRRTs), allowing Member States to help each other to ensure higher level of cyber resilience and to collectively detect, recognise and mitigate cyber threats; calls on the Commission and Member States to build on the PESCO projects on national CRRTs and on mutual assistance in cyber security by establishing a European CRRT tasked with coordinating, detecting and countering collective cyber threats in support of the participating Member States' efforts;

10. Notes that the EU's capability to develop cyber defence projects hinges on its control of technologies, equipment, services, data and data processing, and on its reliance on a trusted industry stakeholder base;

11. Recalls that one aim of the effort to improve the homogeneity of command systems is to ensure that the available command assets are interoperable with those of non-EU NATO countries, as well as with those of occasional partners, and to guarantee a smooth exchange of information so as to speed up the decision-making loop and keep control of information in a cyber-risk context;

12. Recommends that ways be found to complement NATO Smart Defence projects (e.g. the Multinational Cyber Defence Capability Development, the Malware Information

Sharing Platform (MISP) and the Multinational Cyber Defence Education & Training (MNCDE&T));

13. Recognises the developments being made in areas such as nanotechnology, artificial intelligence, big data, e-waste and advanced robotics; urges the Member States and the EU to give particular attention to the possible exploitation of these areas by hostile state actors and organised crime groups; calls for the development of training and capabilities aimed at protecting against the emergence of sophisticated criminal schemes such as complex identity frauds and the counterfeiting of goods;

14. Emphasises the need for more terminological clarity about security in cyber space, as well as for a comprehensive and integrated approach, and joint efforts, to counter cyber and hybrid threats, to detect and eradicate online extremist and criminal safe havens, by strengthening and increasing information sharing between the EU and EU agencies such as Europol, Eurojust, EDA and ENISA;

15. Underlines the growing role of artificial intelligence in both cyber offence as well as defence; urges the EU and the Member States to pay special attention to this area, both in the course of research and in the practical development of their cyber defence capabilities;

16. Strongly emphasises that with the deployment of unmanned aerial vehicles, whether armed or not, additional measures should be taken to reduce their potential cyber vulnerabilities;

Cyber defence of CSDP missions and operations

17. Emphasises that cyber defence should be considered an operational task for CSDP missions and operations, and that it should be included in all CSDP planning processes to ensure that cyber security is constantly considered throughout the planning process, thereby reducing cyber vulnerability gaps;

18. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise as well secure IT infrastructure and networks, both at operational headquarters and within the mission itself, in order to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen the cyber defence expertise provided to EU missions and operations; notes that there is a limit to how well any CSDP mission can be prepared to protect itself from cyber attacks;

19. Stresses that all CSDP mission and operation planning needs to be accompanied by a thorough assessment of the cyber threat-landscape; notes that the threat taxonomy prepared by ENISA provides a suitable template for such an assessment; recommends the creation of a cyber-resilience assessment capability for CSDP HQs;

20. Recognises, in particular, the importance of keeping the cyber footprints and attack surfaces of CSDP missions and operations to the necessary minimum; urges the planners involved to take this into account from the start of the planning process;

21. Acknowledges the EDA Training Needs Analysis, which has brought up major shortfalls in cyber defence skills and competencies among decision makers, not only in the Member States, and welcomes the EDA initiatives on senior decision maker courses within Member States in support of CSDP mission and operation planning;

Cyber defence education and training

22. Notes that a streamlined EU cyber defence education and training landscape would significantly mitigate threats, and calls on the EU and the Member States to increase their cooperation in education, training and exercises;

23. Strongly supports the Military Erasmus Programme and other common training and exchange initiatives aimed at enhancing the interoperability of the armed forces of the Member States and the development of a common strategic culture through an increased exchange of young military personnel, bearing in mind that such interoperability is necessary among all Member States and NATO allies; believes, however, that exchanges for training and education in the field of cyber defence should go beyond this initiative and include military personnel of all ages and from all ranks as well as students from all academic centres of study on cyber security;

24. Stresses that there is a need for more experts in the cyber defence domain; calls on the Member States to facilitate cooperation between civil academic institutions and military academies to bridge this gap with a view to creating more possibilities in the field of cyber defence education and training, and to devote more resources to specialised cyber operational training, including on artificial intelligence; calls on the military academies to integrate cyber defence education into their curricula, thereby helping to increase the cyber talent pool available for CSDP mission needs;

25. Calls on all Member States to sufficiently and proactively inform, raise awareness and advise companies, schools and citizens about cyber security and the main digital threats; welcomes, in this regard, cyber guides as a tool to guide citizens and organisations towards a better cyber security strategy, boost cyber security knowledge and improve cyber resilience across the board;

26. Notes that, given the need for more specialised personnel, the focus of the Member States should not only be on recruitment of competent armed forces personnel, but also on the retention of needed specialists;

27. Welcomes the implementation – by 11 member states (Austria, Belgium, Germany, Estonia, Greece, Finland, Ireland, Latvia, the Netherlands, Portugal and Sweden) of the Cyber Ranges Federation project – of the first of four cyber defence projects launched under the EDA Pooling and Sharing agenda; calls on the other Member States to join this initiative; calls on the Member States to promote greater mutual availability of virtual cyber defence training and cyber ranges; notes, in this regard, that the role of ENISA and its expertise should be also considered;

28. Believes that such initiatives contribute to improving the quality of education in the cyber defence field at EU level, in particular through the creation of wide-ranging technical platforms and the establishment of a community of EU experts; believes that European armed forces can broaden their appeal by providing comprehensive cyber

defence training to attract and retain cyber talent; stresses the need to identify weaknesses in the computer systems of both the Member States and the EU institutions; recognises that human error is one of the most frequently identified weaknesses in cyber security systems, and calls, therefore, for regular training of both military and civilian personnel working for EU institutions;

29. Calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform (CD TEXP) to support the Cyber Ranges Federation as soon as possible, with a focus on strengthening cooperation on harmonised requirements, fostering cyber defence research and technology innovations, and collectively assisting third countries in building their capacities to create resilience in cyber defence; calls on the Commission and the Member States to complement these initiatives with a dedicated European centre of excellence for cyber defence training to provide expert training for the most promising recruits, in support of the participating Member States' cyber training;

30. Welcomes the establishment, within the ESDC, of the Cyber Defence Education, Training Exercise and Evaluation Platform (ETEE) with a view to upscaling the training and education opportunities within the Member States;

31. Encourages more exchanges of situational awareness through table-top cyber exercises and the coordination of respective capability-development efforts in order to achieve greater interoperability and better prevention and response to future attacks; calls for such projects to be conducted with NATO allies, the armed forces of EU Member States and other partners with extensive experience in countering cyber attacks in order to develop operational readiness, common procedures and standards to comprehensively face different cyber threats; welcomes, in this regard, the EU's involvement in cyber exercises such as the Cyber Offence and Defence Exercise (CODE);

32. Recalls that resilient cyber space requires impeccable cyber hygiene; calls on all public and private stakeholders to conduct regular cyber hygiene trainings for all members of their staff;

33. Recommends that the exchange of expertise and lessons learned be increased between the armed forces, police forces and other state bodies of the Member States actively involved in the fight against cyber threats;

EU-NATO cooperation on cyber defence

34. Reiterates that, on the basis of their common values and strategic interests, the EU and NATO have a special responsibility and capacity to address the increasing cyber security and cyber defence challenges more efficiently, and in close cooperation, by looking for possible complementarities, avoiding duplication and acknowledging their respective responsibilities;

35. Calls on the Council, working with other relevant EU institutions and structures, to consider ways of providing, at soon as possible, Union-level support for integrating the cyber domain into Member States military doctrines, in a harmonised manner and in close cooperation with NATO;

36. Calls for the implementation of those measures that have already been agreed upon; calls for new initiatives to further cooperation between EU and NATO to be identified, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and the NATO Communications and Information (NCI) Academy, which aim to increase cyber defence training capabilities in IT and cyber systems, as regards both software and hardware; notes that this could include a dialogue with NATO on the possibility of the EU joining the CCD COE with a view to increasing complementarity and collaboration; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats; urges all relevant institutions and allies to regularly discuss their activities in order to avoid overlaps and encourage a coordinated approach towards cyber defence; believes that it is crucial to stimulate, on the basis of mutual trust, the exchange of cyber threat information among the Member States and with NATO;

37. Is convinced that increased cooperation between EU and NATO is important and useful in the area of cyber defence as a means to prevent, detect and deter cyber attacks; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular in the form of joint exercises and training for civilian and military cyber defence staff and through the participation of Member States in NATO smart defence projects; considers it vital that the EU and NATO step up the sharing of information in order to enable the formal attribution of cyber attacks, and consequently enable the imposition of restrictive sanctions to those responsible; urges both organisations to cooperate more closely as well on the cyber aspects of crisis management;

38. Welcomes the exchange of concepts for integrating cyber defence requirements and standards into the planning and conduct of missions and operations with the aim of fostering interoperability, and expresses the hope that this will be followed up by more operational cooperation to ensure the cyber defence aspect of respective missions and the synchronisation of operational approaches;

39. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT-EU) and the NATO Computer Incident Response Capability (NCIRC), aimed at facilitating the exchange of information, logistical support, shared threat assessments, personnel acquisition and the sharing of best practices, all to ensure the ability to respond to threats in real time; stresses that it is important to encourage information exchanges between CERT-EU and NCIRC and to work towards increasing the level of trust; believes that there is an assumption that information held by CERT-EU could be of use to cyber defence research and to NATO, and that this information should therefore be shared, provided that full conformity with EU data protection legislation is ensured;

40. Welcomes the cooperation between the two organisations on cyber defence exercises; notes the participation of EU representatives in the annual Cyber Coalition Exercise; recognises the progress that the EU's participation – via the Parallel and Coordinated Exercises (PACE) 17 in NATO Crisis Management Exercise 17 – represents, and welcomes, in particular, the inclusion of a cyber defence component; urges both organisations to intensify these efforts;

41. Urges the EU and NATO to organise regular strategic level exercises with the participation of the top political leadership of both organisations; welcomes, in this regard, the Estonian exercise EU CYBRID 2017 where, for the first time, the Secretary General of NATO participated in an EU exercise;

42. Notes that there is substantial scope for a more ambitious and concrete cyber defence cooperation programme that goes beyond the conceptual level of cooperation in the context of specific operations; urges both organisations to implement, in practice and effectively, all that already exists, and to present more ambitious proposals for the next review of the implementation of the Joint Statement;

43. Welcomes the NATO Industry Cyber Partnership (NICP), established in 2014, and calls for EU engagement in cooperative NICP efforts with a view to connecting the NATO-EU cooperation effort with that of industry leaders specialised in cyber technologies with the aim of advancing cyber security through continued collaboration, with particular focus on: training, exercises and education for NATO, EU as well as industry representatives; EU and industry inclusion in NATO Smart Defence projects; collaborative information sharing and best practices for preparedness and recovery between NATO, EU and industry; pursuit of jointly developed capabilities for cyber defence; and collaborative responses to cyber incidents when and where appropriate;

44. Notes the ongoing work on the Proposal for a Regulation revising ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework; calls on ENISA to sign an agreement with NATO to increase their practical cooperation, including the sharing of information and participation in cyber defence exercises;

International norms applicable to cyber space

45. Calls for mainstreaming cyber defence capabilities into the CFSP and the external action of the EU and its Member States as a cross-sectional task, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United Nations, the United States and other strategic partners, in particular as regards rules, norms and enforcement measures in cyber space;

46. Regrets that, after several months of negotiations, the 2016-2017 UN Group of Governmental Experts (UNGGE) was unable to produce a new consensus report; recalls that, as recognised by the 2013 report, existing international law and the United Nations Charter in particular – which prohibits the threat or use of force against the political independence of any state including coercive cyber operations intended to disrupt the technical infrastructure essential to the conduct of official participative procedures, including elections, in another state – applies and should be enforced in cyber space; notes that the 2015 UNGGE report lists a set of norms of responsible state behaviour, including the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules; calls on the EU to assume a leading role in the ongoing and future debates on, and implementation of, international norms in cyber space;

47. Notes the relevance of the Tallinn Manual 2.0 as a basis for a debate and as an analysis of how existing international law can be applied in cyber space; calls on the Member

States to start analysing and applying what the experts have stated in the Tallinn Manual, and to agree on further voluntary norms of international behaviour; notes, in particular, that any offensive use of cyber capabilities should be based on international law;

48. Confirms its full commitment to an open, free, stable and secure cyber space, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means on the basis of the UN Charter and principles of international law; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy and existing cyber norms, and to draw up, together with NATO, EU-level criteria for, and definitions of what constitutes, a cyber attack so as to improve the EU's ability to quickly come to a common position following an internationally wrongful act in the form of a cyber attack; strongly supports the implementation of the 2015 UNGGE report's voluntary, non-binding norms of responsible state behaviour in cyber space, encompassing respect for privacy and the fundamental rights of citizens, and the creation of regional confidence-building measures; supports, in this context, the work of the Global Commission on the Stability of Cyberspace to develop proposals for norms and policies to enhance international security and stability and to guide responsible state and non-state behaviour in cyber space; endorses the proposal that state and non-state actors should not conduct, or knowingly allow, activity that intentionally and substantially damages the general availability or integrity of the public core of the internet, and therefore the stability of cyber space;

49. Recognises that a majority of the technological infrastructure is owned or operated by the private sector and that close cooperation, consultation, and inclusion of the private sector and civil society groups through multi-stakeholder dialogue is therefore essential to ensuring an open, free, stable and secure cyber space;

50. Recognises that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way of complementing multi-stakeholder efforts; stresses the important role that local authorities have to play, in the process of technological innovation and data sharing, when it comes to stepping up the fight against crime and terrorist activities;

51. Welcomes the adoption by the Council of the framework for joint EU diplomatic responses to malicious cyber activities, the so-called EU Cyber Diplomacy Toolbox; supports the possibility for the EU to take restrictive measures against adversaries attacking its Member States in cyber space, including the imposition of sanctions;

52. Calls as well for a clear proactive approach towards cyber security and cyber defence, and for the strengthening of the EU's cyber diplomacy as a cross-sectional task in the EU's foreign policy and its capacities and instruments across the board, so that they can effectively reinforce EU norms and values, as well as pave the way for a consensus on rules, norms and enforcement measures in cyber space globally; notes that building cyber resilience in third countries contributes to international peace and security, ultimately making European citizens safer;

53. Considers that cyber attacks such as NotPetya and WannaCry are either state directed or

are conducted with the knowledge and approval of a state; notes that these cyber attacks, which cause serious and lasting economic damage as well as pose a threat to life, are clear breaches of international law and legal norms; believes, therefore, that NotPetya and WannaCry represent breaches of international law by, respectively, the Russian Federation and North Korea, and that the two countries should face commensurate and appropriate responses from the EU and NATO;

54. Calls for Europol's Cybercrime Centre to become a focal point for law enforcement divisions and government agencies dedicated to cyber crime, the primary responsibility of which would be to manage the defence of both the eu. domains and critical infrastructure of the EU networks during an attack; emphasises that such a focal point should also be mandated to exchange information and provide Member States with assistance;

55. Emphasises the importance of the development of norms regarding privacy and security, encryption, hate speech, disinformation and terrorism threats;

56. Recommends that each Member State embrace the obligations to assist any other Member States under cyber attack and to ensure national cyber accountability in close cooperation with NATO;

Civil-military cooperation

57. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a European single market for cyber security and cyber-security products, based on transparent procedures and in respect of EU and international law, with the view to preserving and strengthening the EU's strategic autonomy; notes the pivotal role that private cyber-security firms play in early warning and attribution of cyber attacks;

58. Strongly emphasises the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the European cyber security industry and other relevant economic actors, to reduce bureaucratic burdens, in particular for SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU to enhance its strategic autonomy; notes, in this context, the valuable contribution that can be made by the EDF and other instruments under the Multiannual Financial Framework (MFF);

59. Encourages the Commission to integrate cyber defence elements into a network of European cybersecurity competence and research centres, also in view of providing sufficient resources to dual use cyber capabilities and technologies within the next MFF;

60. Notes that the protection of public and other civil critical infrastructure assets, in

particular information systems and associated data, is a vital defence task for Member States and, in particular, for the authorities in charge of information systems security, and that it should be part of the remit of either the national cyber defence structures or the said authorities; stresses that this will require a level of trust, and the closest possible cooperation, between military actors, cyber defence agencies, other relevant authorities and the affected industries, which can only be achieved by clearly defining the duties, roles and responsibilities of the civilian and military actors, and urges all stakeholders to take this into account in their planning processes; calls for more cross-border cooperation, with full respect for EU data protection legislation, on law enforcement related to taking down malicious cyber activity;

61. Calls on all Member States to focus national cyber security strategies on the protection of information systems and associated data, and to consider the protection of this critical infrastructure as part of their respective duty of care; urges the Member States to adopt and implement strategies, guidelines and instruments that provide reasonable levels of protection against reasonably identifiable levels of threat, with costs and burdens of the protection proportionate to the probable damage the parties concerned risk facing; calls on the Member States to take appropriate steps to oblige legal persons under their jurisdictions to protect personal data under their care;

62. Recognises that, owing to the changing environment of cyber threats, a stronger and more structured cooperation with police forces could be advisable, especially in some critical areas, e.g. when tracking threats under headings such as cyber *jihad*, cyber terrorism, radicalisation on line and the funding of extremist or radical organisations;

63. Encourages close cooperation between EU agencies such as EDA, ENISA and the European Cybercrime Centre in a cross-sectoral approach aimed at promoting synergies and avoiding overlaps;

64. Calls on the Commission to develop a roadmap for a coordinated approach to European cyber defence, including an update of the EU Cyber Defence Policy Framework to ensure that it remains fit for purpose as the relevant policy mechanism for achieving the EU's cyber defence objectives, in close cooperation with the Member States, the EDA, Parliament and the EEAS; notes that this process has to be part of a broader strategic approach to the CSDP;

65. Calls for cyber security capacity-building through development cooperation, as well as constant education and cyber-awareness training, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries, thus strengthening the resilience of countries and societies *vis-à-vis* cyber and hybrid threats;

66. Calls for international cooperation and multilateral initiatives to build stringent cyber defence and cyber security frameworks to counter state capture by corruption, financial fraud, money laundering, the financing of terrorism, and to tackle the challenges posed by cyber terrorism and by cryptocurrencies and other alternative payment methods;

67. Notes that cyber attacks such as NotPetya spread quickly, thereby causing indiscriminate damage, unless there is widespread resilience globally; believes that cyber defence training and education should form part of the EU's external action and

that building cyber resilience in third countries contributes to international peace and security, ultimately making European citizens safer;

Institutional reinforcement

68. Calls on the Member States to engage in more ambitious cooperation in the cyber domain within PESCO; suggests that the Member States launch a new PESCO cyber cooperative programme with a view to supporting quick and effective planning, command and control of present and future EU operations and missions; notes that this should lead to better coordination of operational capacities in cyber space, and may lead to the development of a common cyber defence command when the European Council so decides;

69. Repeats its call on the Member States and the VP/HR to present an EU white book on security and defence; calls on the Member States and the VP/HR to make cyber defence and deterrence a corner stone of the white book, covering both the protection of the cyber domain for operations laid down in Article 43 TEU and the common defence laid down in Article 42(7) TEU;

70. Notes that the new PESCO cyber cooperative programme should be led by high-ranking military as well as civilian staff from each Member State, on a rotating basis, and be accountable to the EU ministers of defence, in the PESCO format, and to the VP/HR, in order to foster the principles of trust among the Member States and the EU institutions and agencies when sharing information and intelligence;

71. Repeats its call for the creation of an EU Council on Defence based on the existing EDA ministerial Steering Board and the PESCO format of the EU ministers of defence, in order to guarantee the prioritisation and operationalisation of resources, and effective cooperation and integration, among the Member States;

72. Recalls the need to ensure that the European Defence Fund is kept on, or even boosted in the next MFF, with a sufficient budget earmarked for cyber defence;

73. Calls for increased resources to modernise and streamline cyber security and intelligence dissemination between the EEAS/European Union Intelligence and Situation Centre (INTCEN), the Council and the Commission;

Public-private partnerships

74. Recognises that private companies play a key role in preventing, detecting, containing and responding to cyber security incidents, not just as providers of technology but also as providers of non-IT services;

75. Recognises the private sectors role in preventing, detecting, containing and responding to cyber security incidents, along with its role in stimulating innovation in cyber defence, and calls, therefore, for enhanced cooperation with the private sector to ensure shared insights of EU and NATO requirements and assistance in helping to find common solutions;

76. Calls on the EU to perform a comprehensive review of software, IT and

communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programmes and devices, and to ban the ones that have been confirmed as malicious, such as Kaspersky Lab;

77. Instructs its President to forward this resolution to the European Council, the Council, the Commission, the VP/HR, the EU agencies in the fields of defence and cyber security, the NATO Secretary-General and the national parliaments of the Member States.

MINORITY OPINION

On draft report on defence
(2018/2004(INI))

Committee on Foreign Affairs, Rapporteur: Urmas Paet

Minority Opinion tabled by GUE/NGL MEPs Javier Couso Permuy

The report proceed the EU's line of strengthening EU capabilities on cyber defence. It is one example more of EU militaristic and aggressive policy of increasing and reinforcing the military capabilities of EU in Security and Defence defending also the increase of its financing, always in cooperation with NATO.

We object the report since it:

- supports a single market for cybersecurity, promoting synergies and port solutions between the civilian and military markets;

- urges the Member States to use the framework provided by Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) to propose cooperation projects on Cyber defence;

- supports EU-NATO cooperation on defence;

- supports the EU's securitarian and restrictive policy against the rights and freedoms of EU Member States citizens;

- defends the utilization of some instruments under the Multiannual Financial Framework (MFF) for cyber defence;

We demand:

- dissolution of NATO;

- no military funding from EU-budget and strict interpretation of article 41(2) TEU;

- the end of EU Militaristic Policies: PESCO, EDF, the European Defence Industrial Development Programme (EDIDP);

- public funds to support quality jobs, reindustrialization and SMEs;

- strict defence and protection of civil rights and freedoms of all EU's Member States citizens;

- all activities on strictly within UN leadership, UN Charter and International Law;

INFORMATION ON ADOPTION IN COMMITTEE RESPONSIBLE

Date adopted	16.5.2018
Result of final vote	+: 45 –: 8 0: 8
Members present for the final vote	Lars Adaktusson, Michèle Alliot-Marie, Francisco Assis, Petras Auštrevičius, Goffredo Maria Bettini, Elmar Brok, Klaus Buchner, Fabio Massimo Castaldo, Lorenzo Cesa, Aymeric Chauprade, Javier Couso Permuy, Andi Cristea, Arnaud Danjean, Eugen Freund, Sandra Kalniete, Manolis Kefalogiannis, Tunne Kelam, Wajid Khan, Eduard Kukan, Ilhan Kyuchyuk, Arne Lietz, Barbara Lochbihler, Sabine Lösing, Tamás Meszerics, Francisco José Millán Mon, Clare Moody, Javier Nart, Pier Antonio Panzeri, Demetris Papadakis, Ioan Mircea Paşcu, Alojz Peterle, Tonino Picula, Kati Piri, Julia Pitera, Cristian Dan Preda, Jozo Radoš, Michel Reimon, Sofia Sakorafa, Jean-Luc Schaffhauser, Alyn Smith, Dobromir Sośnierz, Jaromír Štětina, Dubravka Šuica, Charles Tannock, László Tőkés, Ivo Vajgl, Geoffrey Van Orden, Boris Zala
Substitutes present for the final vote	David Coburn, Marek Jurek, Norica Nicolai, Urmas Paet, Soraya Post, José Ignacio Salafranca Sánchez-Neyra, Bodil Valero, Marie-Christine Vergiat, Janusz Zemke, Željana Zovko
Substitutes under Rule 200(2) present for the final vote	Renate Weber, Francis Zammit Dimech, Joachim Zeller

FINAL VOTE BY ROLL CALL IN COMMITTEE RESPONSIBLE

45	+
ALDE	Petras Auštrevičius, Ilhan Kyuchyuk, Javier Nart, Norica Nicolai, Urmas Paet, Jozo Radoš, Ivo Vajgl, Renate Weber
EFDD	Fabio Massimo Castaldo, Aymeric Chauprade
PPE	Lars Adaktusson, Michèle Alliot-Marie, Elmar Brok, Lorenzo Cesa, Arnaud Danjean, Sandra Kalniete, Manolis Kefalogiannis, Tunne Kelam, Eduard Kukan, Francisco José Millán Mon, Alojz Peterle, Julia Pitera, Cristian Dan Preda, José Ignacio Salafranca Sánchez-Neyra, Jaromír Štětina, Dubravka Šuica, László Tőkés, Francis Zammit Dimech, Joachim Zeller, Željana Zovko
S&D	Francisco Assis, Goffredo Maria Bettini, Andi Cristea, Eugen Freund, Wajid Khan, Arne Lietz, Clare Moody, Pier Antonio Panzeri, Demetris Papadakis, Ioan Mircea Paşcu, Tonino Picula, Kati Piri, Soraya Post, Boris Zala, Janusz Zemke

8	-
ECR	Geoffrey Van Orden
EFDD	David Coburn
ENF	Jean-Luc Schaffhauser
GUE/NGL	Javier Couso Permuy, Sabine Lösing, Sofia Sakorafa, Marie-Christine Vergiat
NI	Dobromir Sośnierz

8	0
ECR	Marek Jurek, Charles Tannock
VERTS/ALE	Klaus Buchner, Barbara Lochbihler, Tamás Meszerics, Michel Reimon, Alyn Smith, Bodil Valero

Key to symbols:
+ : in favour
- : against
0 : abstention