



2020/2256(INI)

28.4.2021

AMENDMENTS

1 - 257

Draft report
Urmas Paet
(PE689.479v01-00)

State of EU cyber defence capabilities
(2020/2256(INI))

Amendment 1
Ioan-Rareş Bogdan

Motion for a resolution
Citation 11 a (new)

Motion for a resolution

Amendment

— *having regard to the Council conclusions of 22 March 2021 on the EU's Cybersecurity Strategy for the Digital Decade,*

Or. en

Amendment 2
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Citation 18 a (new)

Motion for a resolution

Amendment

— *having regard to the Council conclusions on the EU's Cybersecurity Strategy for the Digital Decade of 9 March 2021,*

Or. en

Amendment 3
Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution
Citation 18 a (new)

Motion for a resolution

Amendment

— *having regards the Declaration of the European Council of 25 March 2021,*

Or. en

Amendment 4

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution

Citation 18 b (new)

Motion for a resolution

Amendment

— *having regards the Open Ended Working Group (OEWG) report of 10 March 2021,*

Or. en

Amendment 5

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Citation 18 b (new)

Motion for a resolution

Amendment

— *having regard to the UN Agenda for Disarmament - Securing our Common Future,*

Or. en

Amendment 6

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Citation 18 c (new)

Motion for a resolution

Amendment

— *having regards to the United Nations Sustainable Development Goals, in particular to SDG 16, aiming at the promotion of peaceful and inclusive societies for sustainable development,*

Or. en

Amendment 7
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Citation 18 d (new)

Motion for a resolution

Amendment

— *having regard to the European Court of Auditors Review No 09/2019 on European Defence,*

Or. en

Amendment 8
David McAllister

Motion for a resolution
Citation 19 a (new)

Motion for a resolution

Amendment

— *having regard to the Council Conclusions on the EU's Cybersecurity Strategy for the Digital Decade of 9 March 2021,*

Or. en

Amendment 9
Assita Kanko

Motion for a resolution
Citation 21 a (new)

Motion for a resolution

Amendment

— *having regard ENISA's the year interview from January 2019 to April 2020,*

Or. en

Amendment 10

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Recital -A (new)

Motion for a resolution

Amendment

-A. whereas the European Union 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”;

Or. en

Amendment 11

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Recital A

Motion for a resolution

Amendment

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

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 civilian domain, and also in the area where both sectors overlap;** **whereas all EU institutions and EU Member States have to work more in common 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 in order to respond to lasting security challenges;

Or. en

Amendment 12
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital A

Motion for a resolution

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

Amendment

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

Or. en

Amendment 13
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital B

Motion for a resolution

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

Amendment

B. 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, **including attacks to disrupt critical infrastructure such as energy, transportation or healthcare; as well as numerous cyber-enabled foreign interferences, which have blurred the limit between peace and hostilities;**

Or. en

Amendment 14
Nicolae Ștefănuță

Motion for a resolution
Recital B

Motion for a resolution

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

Amendment

B. whereas in recent years, we have seen continuous growth in cyber operations conducted by state and non-state actors; ***whereas during the COVID-19 pandemic, the EU and its Member States have observed cyber threats and malicious cyber activities targeting essential operators in Member States and their international partners, including in the health care sector;***

Or. en

Amendment 15
Arnaud Danjean

Motion for a resolution
Recital B

Motion for a resolution

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

Amendment

B. whereas in recent years, we have seen continuous growth in cyber operations conducted by state and non-state actors ***that have revealed vulnerabilities in networks essential to European security; whereas these attacks make it a matter of priority to step up defence capacity and develop European offensive and defensive capabilities;***

Or. fr

Amendment 16
Fabio Massimo Castaldo

Motion for a resolution
Recital B

Motion for a resolution

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

Amendment

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

whereas offensive cyber actors are growing in diversity, sophistication and number, whereas one of the main issues relating to cyberattacks is their poorly identifiable authorship;

Or. en

Amendment 17

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Recital B a (new)

Motion for a resolution

Amendment

B a. whereas cyberspace is considered as the fifth dimension of warfare in addition to land, sea, air and space;

Or. en

Amendment 18

Petras Auštrevičius

Motion for a resolution

Recital C

Motion for a resolution

Amendment

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

C. whereas ***in cyber space there is no clear division between civil and military realms, it is being militarized and weaponized***, conflicts can take place in all physical (land, air, sea and space) and virtual (cyber) domains, and may be amplified through elements of hybrid warfare, proxy wars, offensive and defensive use of cyber capabilities and strategic attacks to disrupt critical infrastructure ***and cause considerable financial losses;***

Or. en

Amendment 19

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution

Recital C

Motion for a resolution

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

Amendment

C. whereas conflicts can take place in all physical (land, air, sea and space) and virtual (cyber) domains, and may be amplified through elements of hybrid warfare, ***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***;

Or. en

Amendment 20

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Recital C

Motion for a resolution

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

Amendment

C. whereas ***cyberspace is now recognized as a domain of operation; whereas the European Union's security environment becomes more complex due to the use of*** elements of hybrid warfare, proxy wars, offensive and defensive cyber capabilities and strategic attacks to disrupt critical infrastructure;

Or. en

Amendment 21

Petras Auštrevičius

Motion for a resolution

Recital C a (new)

Motion for a resolution

Amendment

C a. whereas cyber-attackers are using state-of-the-art technology to investigate vulnerabilities in systems and devices and to engage in large- and mega-scale cyber-attacks;

Or. en

Amendment 22

Petras Auštrevičius

Motion for a resolution

Recital C b (new)

Motion for a resolution

Amendment

C b. whereas the EU is a net importer of cyber security products and services, which increases the risk of technological dependence and vulnerability to non-EU operators;

Or. en

Amendment 23

Petras Auštrevičius

Motion for a resolution

Recital C c (new)

Motion for a resolution

Amendment

C c. whereas cyber espionage and cyber sabotage in cyber space are growing significantly and pose a serious threat;

Or. en

Amendment 24

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Recital D

Motion for a resolution

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

Amendment

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

Or. en

Amendment 25

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Recital D

Motion for a resolution

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

Amendment

D. whereas the European External Action Service (EEAS), the European Commission and 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***;

Or. en

Amendment 26
Fabio Massimo Castaldo

Motion for a resolution
Recital D a (new)

Motion for a resolution

Amendment

D a. whereas the cyber domain, now considered the fifth domain of warfare alongside land, maritime, air and space is wide and encompass everything from information and telecommunication networks, infrastructure and the data they support, to computer systems, processors and controllers and thus an effective cyber defence requires an holistic approach and a high level of cooperation from a wide range of public and private actors and cyber stakeholders from different fields, as well as enhanced cooperation with other like-minded international actors;

Or. en

Amendment 27
Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Recital D a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 28
Fabio Massimo Castaldo

Motion for a resolution
Recital D b (new)

Motion for a resolution

Amendment

D b. whereas, due to the nature of the cyber domain, a proper defence is often at a structural disadvantage in comparison with attacks, especially those of a global or cross border nature and especially in case of fragmentation of strategies and capabilities;

Or. en

Amendment 29
Urmaz Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Recital D b (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 30
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Recital E

Motion for a resolution

Amendment

E. whereas EU Cyber Defence Policy

E. whereas EU Cyber Defence Policy

Framework updated in 2018 identified priorities, including the development of cyber defence capabilities, as well as the protection of the Common Security and Defence Policy's (CSDP) communication and information networks;

Framework updated in 2018 identified priorities, including the development of **military** cyber defence capabilities, as well as the protection of the Common Security and Defence Policy's (CSDP) communication and information networks, **as regards CSDP organisational structures, but also ad hoc structures in the field where civilian and military CSDP missions and operations are deployed;**

Or. en

Amendment 31

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Recital E a (new)

Motion for a resolution

Amendment

E a. whereas the defence and space industries are facing unprecedented global competition and major technological changes with the emergence of advanced cyber technologies;

Or. en

Amendment 32

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Recital F

Motion for a resolution

Amendment

F. whereas the increasing integration of Artificial Intelligence (AI) into defence forces' **offensive cyber** capabilities (cyber-physical systems, including the communication and data links between vehicles in a networked system) may lead

F. whereas the increasing integration of Artificial Intelligence (AI) into **all** defence forces' **military** capabilities (***the so called system behind most weapons systems, which is sensors collecting data, and algorithms processing and analysing***

to vulnerabilities to electronic warfare **attacks** such as jamming, spoofing or hacking;

that data, cyber-physical systems, including the communication and data links between vehicles in a networked system) may lead to vulnerabilities to **conventional and** electronic warfare such as jamming, spoofing or hacking, **which could block or weaken legitimate military action**;

Or. en

Amendment 33
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital F

Motion for a resolution

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

Amendment

F. 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;

Or. en

Amendment 34
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital F a (new)

Motion for a resolution

F a. whereas the European Court of Auditors pointed to capability gaps in the area of ICT technologies, cyber warfare and AI;

Or. en

Amendment 35
Nicolae Ștefănuță

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

G. whereas raising the level of cyber security within the EU is a necessary corollary to the success of Europe's digital ambitions; ***whereas a EU with strong cybersecurity culture and technology would be able to guarantee digital sovereignty, support a strong online economy and protect its citizens;***

Or. en

Amendment 36
Assita Kanko

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

G. whereas raising the level of cyber security within the EU is a necessary corollary to the success of Europe's digital ambitions ***and to keep pace with the growing sophistication and threat of cyberattacks, ransomware and malware;***

Or. en

Amendment 37
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

G. whereas raising the level of cyber security within the EU is a necessary corollary to the success of Europe's digital ambitions; ***as well as the security of its member states;***

Or. en

Amendment 38
David McAllister

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

G. whereas raising the level of cyber security within the EU is a necessary corollary to the success of Europe's digital ambitions ***and would create greater resilience;***

Or. en

Amendment 39
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

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

Or. en

Amendment 40
Fabio Massimo Castaldo

Motion for a resolution
Recital G

Motion for a resolution

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

Amendment

G. whereas raising the level of cyber security within the EU is necessary **for** the success of Europe’s digital ambitions;

Or. en

Amendment 41

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Recital G a (new)

Motion for a resolution

Amendment

G a. whereas one of the goals envisaged by the European Commission proposal for a Regulation of the European Parliament and the Council establishing the “European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres” has been to enhance synergies between the civilian and military dimensions and to increase cooperation between civilian and defence cybersecurity research and innovation communities;

Or. en

Amendment 42

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Recital G a (new)

Motion for a resolution

Amendment

G a. whereas the June 2017 Council Conclusions establishing a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities (“Cyber Diplomacy Toolbox”) showed the added value of a joint EU diplomatic response to malicious cyber activities;

Or. en

Amendment 43
Assita Kanko

Motion for a resolution
Recital G a (new)

Motion for a resolution

Amendment

G a. whereas the world pandemic COVID-19, the world is rapidly changing and the EU Cyber Defense Policy Framework must be updated;

Or. en

Amendment 44
Petras Auštrevičius

Motion for a resolution
Recital G a (new)

Motion for a resolution

Amendment

G a. whereas the EU aims to create the most secure digital environment;

Or. en

Amendment 45
Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Recital G b (new)

G b. whereas different state actors like Russia, China and North Korea 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, 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;

Or. en

Amendment 46

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Recital H

Motion for a resolution

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

Amendment

H. 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 cyber-attacks in order to better prevent, discourage, deter and respond to malicious behavior in cyberspace; whereas the legal framework for ***the EU cyber sanctions regimes*** was adopted in May 2019;

Or. en

Amendment 47

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Recital H a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 48

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Recital I

Motion for a resolution

Amendment

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

I. whereas EU-NATO cooperation has increased across multiple fields, including cyber ***security and*** defence, ***inline with the 2016 EU-NATO Joint Declaration has increased over the past years;***

Or. en

Amendment 49

Assita Kanko

Motion for a resolution

Recital I a (new)

Motion for a resolution

Amendment

I a. whereas the studies published by NATO's Strategic Communications Centre of Excellence outlines the increasingly capable social media bots, A-I created fake images video and weapons

platforms Russia uses;

Or. en

Amendment 50
Fabio Massimo Castaldo

Motion for a resolution
Recital J a (new)

Motion for a resolution

Amendment

J a. whereas EU's ambition to acquire a more prominent geopolitical role by becoming 'strategically autonomous' and 'technologically sovereign' also rests on credible cyber defence and deterrence, including the capacity to identify malicious actions in a timely effective manner and to respond adequately;

Or. en

Amendment 51
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Recital J a (new)

Motion for a resolution

Amendment

J a. whereas damaging cyberattacks can take place at any moment; whereas actors on both European and national levels should be encouraged to take necessary measures to maintain effective cyber defence capabilities even during peacetime;

Or. en

Amendment 52

Assita Kanko

Motion for a resolution

Recital J a (new)

Motion for a resolution

Amendment

J a. whereas hybrid warfare tactics have increased in the last decades; whereas the EU must define a clear position towards this evolving threat;

Or. en

Amendment 53

Assita Kanko

Motion for a resolution

Recital J b (new)

Motion for a resolution

Amendment

J b. whereas international terrorist organizations have increased their expertise in and use of cyber warfare;

Or. en

Amendment 54

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Subheading 1

Motion for a resolution

Amendment

The state of EU cyber defence capabilities

The state of EU ***cooperation on military and civilian*** cyber defence capabilities

Or. en

Amendment 55

Lukas Mandl, Henna Virkkunen

on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 1

Motion for a resolution

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

Amendment

1. Underlines that a common cyber defence policy and a substantial cyber defence capability are core elements for the development of the European Defence Union **and require a complex mix of technical, strategic and operational abilities**; stresses the urgent need to strengthen EU and the Member State cyber defence capabilities; **underlines the key operational capabilities of detection, attribution, and incident response, and underlines in this regard the need of multi-domain-awareness monitoring schemes**;

Or. en

Amendment 56
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 1

Motion for a resolution

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

Amendment

1. Underlines that a common cyber defence policy and substantial **EU level cooperation on generating common and also better national military** cyber capabilities are core elements for the **strengthening of an effective Common Security and Defence Policy and overall resilience of the** Union; stresses the urgent need to **develop and** strengthen **both, common and** Member State **military** cyber defence capabilities;

Or. en

Amendment 57

David Lega

Motion for a resolution

Paragraph 1

Motion for a resolution

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

Amendment

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

Or. en

Amendment 58

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Bart Groothuis

Motion for a resolution

Paragraph 1

Motion for a resolution

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

Amendment

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

Or. en

Amendment 59

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 1

Motion for a resolution

1. Underlines that a common cyber

PE691.415v01-00

Amendment

1. Underlines that a common cyber

26/124

AM\1229723EN.docx

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

defence policy and substantial cyber defence **capabilities** are core elements for the development of the European Defence Union; stresses the urgent need to strengthen EU and the Member State cyber defence capabilities;

Or. en

Amendment 60
Arnaud Danjean

Motion for a resolution
Paragraph 1 a (new)

Motion for a resolution

Amendment

1a. Recalls that responsibility for cyber security rests primarily with the Member States, while the EU has a key role in supporting and developing the cyber defence capabilities of public and private entities within the Member States, coordinating their efforts and harmonising legislation from the top;

Or. fr

Amendment 61
Assita Kanko

Motion for a resolution
Paragraph 1 a (new)

Motion for a resolution

Amendment

1 a. Welcomes the new EU Cybersecurity Strategy announced by the Commission and the High Representative on 16th December 2020; calls on the EU to fully work and cooperate with Member states to prevent cyber-attacks and to establish a cyber defence;

Or. en

Amendment 62
Assita Kanko

Motion for a resolution
Paragraph 1 b (new)

Motion for a resolution

Amendment

1 b. Welcomes the new “European Cybersecurity Industrial, Technology and Research Competence Centre” adopted by the Council in April 2021, and encourages seamless cooperation with its network of national coordination centres;

Or. en

Amendment 63
Assita Kanko

Motion for a resolution
Paragraph 1 c (new)

Motion for a resolution

Amendment

1 c. Supports the creation of an EU External Cyber Capacity Building Agenda that will increase cyber capacity-building efforts to third countries;

Or. en

Amendment 64
Assita Kanko

Motion for a resolution
Paragraph 1 d (new)

Motion for a resolution

Amendment

1 d. Notes that the COVID-19 pandemic and the increase of cyber insecurity demonstrated that international agreements are necessary; Suggest that the European Union could take the role

and promote the creation of international agreements with third countries regarding the data's protection rights;

Or. en

Amendment 65

Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

Motion for a resolution

Paragraph 2

Motion for a resolution

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

Amendment

2. Recalls that the borderless nature of cyber space and the substantial number of cyber-attacks make them a threat requiring intensified ***cooperation between the Member States*** and a coordinated Union-level response, including common Member State support capabilities; ***stresses that individual States, frequently being subject to threats specifically directed at them, are each free to pursue an independent cyber defence strategy, while at the same time envisaging partnerships tailored to their particular concerns;***

Or. fr

Amendment 66

Nicolae Ștefănuță

Motion for a resolution

Paragraph 2

Motion for a resolution

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

Amendment

2. Recalls that the borderless nature of cyber space and the substantial number of cyber-attacks make them a threat requiring intensified EU-NATO cooperation ***based on coordinated efforts to counter hybrid threats, information sharing between cyber crisis response teams, exchange of best practices, enhanced training,***

research and exercises and a coordinated Union-level response, including common Member State support capabilities;

Or. en

Amendment 67

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution **Paragraph 2**

Motion for a resolution

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

Amendment

2. Recalls that the borderless nature of cyber space *as well as* the substantial number *and increasing complexity* of cyber-attacks *require* intensified EU-NATO cooperation and a coordinated Union-level response, including common Member State support capabilities *and Member State support for measures of the EU's cyber diplomacy toolbox*;

Or. en

Amendment 68

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution **Paragraph 2**

Motion for a resolution

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

Amendment

2. Recalls that the borderless nature of cyber space *as well as* the substantial number *and increasing complexity* of cyber-attacks *require* a coordinated Union-level response, including common Member *States* support capabilities, *as well as intensified international cooperation, among them between the EU and NATO*;

Or. en

Amendment 69
Emmanuel Maurel

Motion for a resolution
Paragraph 2

Motion for a resolution

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

Amendment

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

Or. fr

Amendment 70
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 2 a (new)

Motion for a resolution

2 a. Believes that in order to ensure an all-encompassing resilience, it is necessary not only to strengthen technological infrastructures and to possess response capabilities, but also to spread a cyber security culture among the population;

Amendment

2 a. *Believes that in order to ensure an all-encompassing resilience, it is necessary not only to strengthen technological infrastructures and to possess response capabilities, but also to spread a cyber security culture among the population;*

Or. en

Amendment 71
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 3

Motion for a resolution

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

Amendment

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

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

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

Or. en

Amendment 72

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 3

Motion for a resolution

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

Amendment

3. ***Welcomes the CDPF as a tool to support the development of EU Member States cyber defence capabilities;*** Stresses that the review of the Cyber Defence Policy Framework (CDPF) should enhance coordination between EU ***institutions, agencies and bodies***, between and with Member States, as well as with the European Parliament, in order to ensure the updated CDPF achieves the EU's cyber defence objectives;

Or. en

Amendment 73

Nicolae Ștefănuță

Motion for a resolution

Paragraph 3 a (new)

Motion for a resolution

Amendment

3 a. Welcomes the decision of the Council to give green light for the establishment of the European Cybersecurity Industrial, Technology and Research Competence Centre in Bucharest, Romania, which will work together with a network of national coordination centres designed by Member States and with the European Union Agency for Cybersecurity and which will channel cybersecurity-related funding from Horizon Europe and the Digital Europe Programme; 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 form a cybersecurity competence community with the aim to enhance and spread cybersecurity expertise across the EU;

Or. en

Amendment 74
Assita Kanko

Motion for a resolution
Paragraph 3 a (new)

Motion for a resolution

Amendment

3 a. Highlights that the Commission and Member states should cooperate with the European Agencies as for example, the European Cyber Security Organisation (ECSO), the European Union Agency for Cybersecurity (ENISA), European Union Agency for Law Enforcement Cooperation (EUROPOL), European Defence Agency (EDA), European Space Agency (ESA);

Or. en

Amendment 75

Assita Kanko

Motion for a resolution

Paragraph 3 b (new)

Motion for a resolution

Amendment

3 b. Considers that the Commission and Member states should have a further cooperation with Europol as it faces cyber-security threats; considering that Europol set out the European Cybercrime Centre (EC3) in 2013 to protect EU citizens and to strengthen the law enforcement response to cybercrime in the EU;

Or. en

Amendment 76

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 4

Motion for a resolution

Amendment

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination; **urges a cooperation strategy with** the EU's Computer Emergency Response Teams (CERT-EU) **to protect** networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU **results to ensured** a level of IT security that will allow it to receive all the necessary classified and non-classified information to carry out its responsibilities under the Treaties, including as a result of the current process to replace the 2002 Inter-Institutional Agreement on access to information in the area of security and defence;

4. Calls on the EEAS **and the European Commission, in cooperation with the Member States**, to further develop a coherent IT security policy to strengthen cyber defence coordination; **notes that** the EU's Computer Emergency Response Teams (CERT-EU) **is responsible for the protection of** networks used by all EU institutions, **bodies and agencies, in close cooperation with CIOs in the respective entities**; calls on the European Parliament to ensure its participation in CERT-EU, **which would guarantee** 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 the adequate levels of cybersecurity for the EEAS assets, premises and activities, including the headquarters, EU delegations and CSDP missions and operations;***

Or. en

Amendment 77

Lukas Mandl, Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution

Paragraph 4

Motion for a resolution

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

Amendment

4. Calls on the EEAS ***and the European Commission, in cooperation with the Member States*** to further develop ***comprehensive set of measures and a coherent IT security policy to strengthen cyber defence and resilience*** coordination; urges a cooperation strategy with the EU's Computer Emergency Response Teams (CERT-EU) to protect networks used by all EU institutions ***bodies and agencies; improve information sharing on technical information, analysis and threat intelligence between Member States at EU-level that could enable collective attribution on EU-level;*** calls on the European 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;

Or. en

Amendment 78
Nicolae Ștefănuță

Motion for a resolution
Paragraph 4

Motion for a resolution

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

Amendment

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination, ***while focusing on prevention, detection, incident response, situational awareness, information exchange and early warning mechanism***; urges a cooperation strategy with the EU's Computer Emergency Response Teams (CERT-EU) to protect networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU results to 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;

Or. en

Amendment 79
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 4

Motion for a resolution

4. Calls on the EEAS to further develop a coherent IT security policy ***to*** strengthen cyber defence coordination; urges a cooperation strategy with the EU's Computer Emergency Response Teams

Amendment

4. Calls on the EEAS to further develop a coherent IT security policy ***and to first of all*** strengthen ***resilience, but also military*** cyber defence coordination; urges a cooperation strategy with the EU's

(CERT-EU) to protect networks used by all EU institutions; calls on the European 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;

civilian Computer Emergency Response Teams (CERT-EU) to protect networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU results to 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;

Or. en

Amendment 80
David McAllister

Motion for a resolution
Paragraph 4

Motion for a resolution

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

Amendment

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination; urges a cooperation strategy with the EU's Computer Emergency Response Teams (CERT-EU) to protect networks used by all EU institutions ***and its communication with Member States***; calls on the European 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;

Or. en

Amendment 81

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 4

Motion for a resolution

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination; urges **a** cooperation **strategy** with the EU's Computer Emergency Response **Teams** (CERT-EU) to protect networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU results to ensured a level of IT security that will allow it to receive all the necessary classified and non-classified information to carry out its responsibilities under the Treaties, including as a result of the current process to replace the 2002 Inter-Institutional Agreement on access to information in the area of security and defence;

Amendment

4. Calls on the EEAS to further develop a coherent IT security policy to strengthen cyber defence coordination; urges **to strengthen** cooperation with the EU's Computer Emergency Response **Team** (CERT-EU) to protect networks used by all EU institutions; calls on the European Parliament to ensure its participation in CERT-EU results to ensured a level of IT security that will allow it to receive all the necessary classified and non-classified information to carry out its responsibilities under the Treaties, including as a result of the current process to replace the 2002 Inter-Institutional Agreement on access to information in the area of security and defence;

Or. en

Amendment 82

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution

Paragraph 5

Motion for a resolution

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

Amendment

5. Notes the 2018 CDPF's objective to setup an EU Military CERT-Network; **welcomes the launch of Cyber Crises Liaison Organisation Network (CyCLONe) on 29 September 2020, which further improved ability for timely information sharing and situational awareness by closing the gap between**

*EU's technical and political levels; calls on **the EU** Member States to significantly increase classified information sharing, to develop a European rapid and secure network to counter cyber-attacks; **also notes that an effective cyber defence capability requires a change from “Need-to-know” based culture of information sharing into a “Need-to-share” one;***

Or. en

Amendment 83
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 5

Motion for a resolution

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

Amendment

5. Notes the 2018 CDPF's objective to setup an EU Military CERT-Network; calls on **the EU** Member States to significantly increase information sharing, to develop a European rapid and secure network to counter cyber-attacks; **acknowledges the launch of the information sharing and situational awareness platform - Cyber Crises Liaison Organisation Network (CyCLONe) on 29 September 2020;**

Or. en

Amendment 84
Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

Motion for a resolution
Paragraph 5

Motion for a resolution

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

Amendment

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

counter cyber-attacks;

network to counter cyber-attacks; ***stresses that each country has the right to protect its information for imperative reasons of national security;***

Or. fr

Amendment 85

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution

Paragraph 5

Motion for a resolution

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

Amendment

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, when needed and useful,*** and to develop a European rapid and secure network to counter cyber-attacks;

Or. en

Amendment 86

Petras Auštrevičius

Motion for a resolution

Paragraph 5

Motion for a resolution

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

Amendment

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

Or. en

Amendment 87
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 5 a (new)

Motion for a resolution

Amendment

5 a. Calls on every Member State, to adopt policies able to develop a coherent and cyberthreat intelligence approach in order to have a situation awareness on cyberattack, that include an enhancement Permanent Structured Cooperation (PESCO) and adoption of EU Cyber Intelligence Center in cooperation with every Member State;

Or. en

Amendment 88
Emmanuel Maurel

Motion for a resolution
Paragraph 5 a (new)

Motion for a resolution

Amendment

5a. Is concerned at the Sino-American duopoly established in key digital technologies;

Or. fr

Amendment 89
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 6

Motion for a resolution

Amendment

6. Recalls that the 2018 EU Capability Development Priorities (CDP) made cyber

6. Recalls that the 2018 EU Capability Development Priorities ***established in the***

defence a key priority; welcomes *the EDA's projects to improve overall EU Member States efforts in this field*; takes note of *the EDA's CyDRE project, which should develop an enterprise architecture for cyberspace operations*, including *scope, functionalities and requirements, based upon national and EU legislation*;

framework of the Capability Development Plan (CDP) made cyber defence a key priority (i.e. "enabling capabilities for cyber responsive operations"); welcomes *EDA for supporting Member States in developing their capabilities to improve cyber resilience, as the ability to detect, withstand and recover from any cyber attack* ; takes note of *different activities undertaken by Member States in the framework of EDA* including *by promoting best practices in system engineering framework for cyber operations to harmonize the design and development of national cyber defence capabilities following a shared vision through the 'Cyber Defence Requirements Engineering' (CyDRE) project*;

Or. en

Amendment 90

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 6

Motion for a resolution

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

Amendment

6. Recalls that the 2018 EU Capability Development Priorities (CDP) ***reflected on the need to develop full-spectrum capabilities and*** made cyber defence ***capabilities as*** a key priority; ***reminds that the CDP underlined that cyber situational awareness technologies and defensive cyber technologies are essential to counter security threats to the EU and Member States' command and control structures***; welcomes the EDA's projects to improve overall EU Member States efforts in this field; takes note of the EDA's CyDRE project which should develop an enterprise architecture for cyberspace operations, including scope, functionalities and requirements based upon national and EU legislation;

Amendment 91
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 6 a (new)

Motion for a resolution

Amendment

6 a. *Notes the 2018 CDPF's objective to setup an EU Military CERT-Network and the Directive on security of network and information systems (NIS), calls on Member States to significantly increase of information sharing method, to define a common communication standard that could be used for classified and non-classified information, in order to enhanced the rapid action and secure network to counter cyber-attacks;*

Or. en

Amendment 92
Assita Kanko

Motion for a resolution
Paragraph 6 a (new)

Motion for a resolution

Amendment

6 a. *Stresses that cyber-attacks have increased throughout the EU in the last year during the COVID-19 pandemic and that such attacks are increasingly sophisticated among both state and non-state actors; calls for the European Commission and Member states to take further actions in the cyber-defence capabilities;*

Or. en

Amendment 93

Assita Kanko

Motion for a resolution

Paragraph 6 b (new)

Motion for a resolution

Amendment

6 b. Highlights that in the recent years, the European Medicines Agency (EMA) has been cyber attacked; underlines that other Member states have also witnessed cyber-attacks in the recent years;

Or. en

Amendment 94

Assita Kanko

Motion for a resolution

Paragraph 6 c (new)

Motion for a resolution

Amendment

6 c. Notes that there is an external growth cyber-attacks, where China, North Korea and Russia have been the actors;

Or. en

Amendment 95

Lukas Mandl, Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution

Paragraph 7

Motion for a resolution

Amendment

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

7. **Welcomes** the Coordinated Annual Review on Defence (CARD) – **a first fully fledged defence review at EU level, which** is a key tool that supports **the** overall coherence in Member States' defence **spending, defence** planning **and defence**

cooperation, and should contribute to promoting investment in *developing cyber* defence capabilities;

Or. en

Amendment 96
David McAllister

Motion for a resolution
Paragraph 7

Motion for a resolution

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

Amendment

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

Or. en

Amendment 97
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 8

Motion for a resolution

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

Amendment

8. *Reminds that the EDIDP included intelligence, secured communication and cyber-defence in its work programmes; particularly welcomes the call for Easily deployable and interconnected cyber toolbox for defence;* notes that the European Defence Fund (EDF), will also support strengthening resilience, and improve preparedness, responsiveness and cooperation in the cyber domain;

Or. en

Amendment 98
Nicolae Ștefănuță

Motion for a resolution
Paragraph 8

Motion for a resolution

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

Amendment

8. Notes that the European Defence Fund (EDF), will also support strengthening resilience, and improve preparedness, responsiveness and cooperation in the cyber domain; ***calls on the Member States to take advantage of the EDF to jointly develop cyber defence capabilities;***

Or. en

Amendment 99
Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution
Paragraph 8

Motion for a resolution

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

Amendment

8. ***Welcomes the progress already made under the EDIDP with several relevant projects, and the fact*** that the European Defence Fund (EDF) will also support strengthening resilience and improve preparedness, responsiveness and cooperation in the cyber domain;

Or. en

Amendment 100
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 8

Motion for a resolution

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

Amendment

8. Notes that the European Defence Fund (EDF), ***may*** support strengthening resilience, and improve preparedness, responsiveness and cooperation in the cyber domain ***provided such a priority will be decided when negotiating relevant EDF work programmes;***

Or. en

Amendment 101
David McAllister

Motion for a resolution
Paragraph 8

Motion for a resolution

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

Amendment

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

Or. en

Amendment 102
Arnaud Danjean

Motion for a resolution
Paragraph 8 a (new)

Motion for a resolution

8a. Stresses that EU capability to develop cyber defence projects depends on control of technologies, equipment, services, data and data processing and has to rely on a trusted sectoral stakeholder base;

Or. fr

Amendment 103
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 9

Motion for a resolution

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

Amendment

9. Welcomes the progress achieved by the Permanent Structured Cooperation (PESCO), ***including by implementing concrete projects such as*** Cyber Rapid Response Team ***and Mutual Assistance in Cybersecurity project***; recalls that PESCO ***through the more binding commitments as well as different projects taken forward in PESCO framework*** offers excellent ways to speed up cyber security initiatives, such as through the Cyber Threats and Incident Response Information Sharing Platform and Cyber and Information Domain Coordination Centre;

Or. en

Amendment 104
Petras Auštrevičius

Motion for a resolution
Paragraph 9

Motion for a resolution

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

Amendment

9. Welcomes the progress achieved by the Permanent Structured Cooperation (PESCO) Cyber Rapid Response ***Teams and Mutual Assistance in Cyber Security (CRRTs) project led by Lithuania and encourages the active participation of all other EU Member States***; recalls that PESCO offers excellent ways to speed up cyber security initiatives, such as through the Cyber Threats and Incident Response Information Sharing Platform and Cyber and Information Domain Coordination Centre;

Amendment 105
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 9

Motion for a resolution

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

Amendment

9. Welcomes the ***increased cooperation among Member States in the domain of cyber defence and C4ISR in the framework of*** the Permanent Structured Cooperation (PESCO), ***including*** Cyber Rapid Response ***Teams and Mutual Assistance in Cybersecurity project***; recalls that PESCO offers excellent ways to speed up cyber security initiatives, such as through the Cyber Threats and Incident Response Information Sharing Platform and Cyber and Information Domain Coordination Centre;

Or. en

Amendment 106
Nicolae Ștefănuță

Motion for a resolution
Paragraph 9

Motion for a resolution

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

Amendment

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

Amendment 107

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution

Paragraph 9

Motion for a resolution

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

Amendment

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

Or. en

Amendment 108

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 9 a (new)

Motion for a resolution

Amendment

9 a. Recalls that the successful implementation 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;

Or. en

Amendment 109
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 9 a (new)

Motion for a resolution

Amendment

9 a. Welcomes the Council's Decision of 5 November 2020, allowing third countries (non-EU Member States) to join PESCO projects given that they can add value and meet political, substantive and legal conditions; invites EU Member States and non-EU Member States to participate in PESCO cyber related projects;

Or. en

Amendment 110
Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță,
Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Paragraph 9 a (new)

Motion for a resolution

Amendment

9 a. 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;

Or. en

Amendment 111
Assita Kanko

Motion for a resolution
Paragraph 9 a (new)

Motion for a resolution

Amendment

9 a. Welcomes the new Quantum Technologies Flagship; notes that the Union must do further action regarding quantum computing as other countries are predominant on this concern;

Or. en

Amendment 112

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution Paragraph 10

Motion for a resolution

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

Amendment

10. Emphasises that in line with the Civilian CSDP Compact, civilian CSDP must be cyber resilient and support third countries' **cyber capacity-building** including through Monitoring, Mentoring, and Advice; **recommends to explore options to foster the cyber capability-building of our partners such as extending the mandate of EU Training Missions to also comprise cyber defence aspects or to launch Civilian cyber missions;**

Or. en

Amendment 113

David McAllister

Motion for a resolution Paragraph 10

Motion for a resolution

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

Amendment

10. 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;

Or. en

Amendment 114
Petras Auštrevičius

Motion for a resolution
Paragraph 11

Motion for a resolution

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

Amendment

11. Welcomes the Council's June 2019 framework, which allows targeted restrictive measures to deter and respond to cyber-attacks that constitute a threat to the EU or its Member States, including cyber-attacks against third countries or international organisations; welcomes the imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox; ***notes the prevailing lack of legal norms to contain cyber-attacks by state and non-state actors, and calls for further development and strict enforcement of a system of proportionate punishments;***

Or. en

Amendment 115
Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

Motion for a resolution
Paragraph 11

Motion for a resolution

11. Welcomes the Council's June 2019 framework, which allows targeted restrictive measures to deter and respond to cyber-attacks that constitute a threat to the EU or its Member States, including cyber-attacks against third countries or international organisations; welcomes the

Amendment

11. Welcomes the Council's June 2019 framework, which allows targeted restrictive measures to deter and respond to cyber-attacks that constitute a threat to the EU or its Member States, including cyber-attacks against third countries or international organisations; welcomes the

imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox;

imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox; ***notes that digital freedom of expression must be an absolute imperative and be factored into cyber security initiatives accordingly;***

Or. fr

Amendment 116

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 11

Motion for a resolution

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

Amendment

11. Welcomes the ***Council Decision of 14 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States***, which allows targeted restrictive measures to deter and respond to cyber-attacks that constitute a threat to the EU or its Member States, including cyber-attacks against third countries or international organisations; welcomes the imposition of such restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox;

Or. en

Amendment 117

Lukas Mandl, Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution

Paragraph 11

Motion for a resolution

Amendment

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

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

Or. en

Amendment 118

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 11

Motion for a resolution

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

Amendment

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

Or. en

Amendment 119

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 11 a (new)

Motion for a resolution

Amendment

11 a. Notes the imposition of restrictive measures in July 2020 and October 2020 as a credible step in strengthening the EU's cyber diplomacy toolbox, while respecting the European vision for the internet, which is one of a single, open, neutral, free, secure and un-fragmented network;

Or. en

Amendment 120

Assita Kanko

**Motion for a resolution
Paragraph 11 a (new)**

Motion for a resolution

Amendment

11 a. Recognises that machine-learning systems can use sensor data, entire technical libraries and advanced models to accurately predict and prevent equipment failure and should thus be integrated into our procurement plans;

Or. en

Amendment 121

Juozas Olekas, Attila Ara-Kovács

**Motion for a resolution
Paragraph 11 a (new)**

Motion for a resolution

Amendment

11 a. Welcomes the plans to establish EU cyber intelligence working group within EU intelligence and Situation Centre (INTCEN) to advance strategic intelligence cooperation on cyber threats;

Or. en

Amendment 122

Assita Kanko

Motion for a resolution

Paragraph 11 b (new)

Motion for a resolution

Amendment

11 b. Recommends an audit be taken by the EU to better understand what European forces need, where the key shortfalls are found and the level of resource-waste caused by redundant fixed assets and duplication of effort;

Or. en

Amendment 123

Assita Kanko

Motion for a resolution

Paragraph 11 c (new)

Motion for a resolution

Amendment

11 c. Reminds that the European Union discussed in the International Summit held in June 2020 with China, about global challenges such as the raising issues in cybersecurity and disinformation;

Or. en

Amendment 124

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 12

Motion for a resolution

Amendment

12. Welcomes the work led by ENISA involving the Member States and interested stakeholders to provide the EU with

12. Recalls that given the dual nature of cybertechnologies, secured civilian products and services are key to the

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;

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

Or. en

Amendment 125

Lukas Mandl, Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution

Paragraph 12

Motion for a resolution

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

Amendment

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

Or. en

Amendment 126
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 12 a (new)

Motion for a resolution

Amendment

12 a. Underlines the importance of investments in cyber-defence and cybersecurity capabilities with the aim to enhance EU's and its Member States' resilience and strategic capacities, highlights in this regard the importance of Digital Europe Programme and Horizon Europe, especially its Civil Security for Society'cluster; notes the significance of relevant financial instruments available within the 2021-2027 Multiannual Financial Framework (MFF) as well as in the Recovery and Resilience Facility (RRF);

Or. en

Amendment 127
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 12 a (new)

Motion for a resolution

Amendment

12 a. Welcomes the progress made by some EU Members States in establishing cyber commands within their military;

Or. en

Amendment 128
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group

Rasa Juknevičienė

**Motion for a resolution
Paragraph 12 b (new)**

Motion for a resolution

Amendment

12 b. *Notes that the number of cyber-attacks has significantly increased during the Covid-19 pandemic and welcomes that the Recovery Plan for Europe foresees additional investments in cybersecurity;*

Or. en

Amendment 129

Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

**Motion for a resolution
Paragraph 13**

Motion for a resolution

Amendment

13. *Notes that the Strategic Compass will enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into capability needs, including in cyber defence, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;*

13. *Points out that, with regard to cyber defence and defence in general, national interests must take precedence and that notions of European sovereignty extending into this domain must in no way induce a Member State to accept provisions contrary to its fundamental interests regarding defence and national security;*

Or. fr

Amendment 130

Markéta Gregorová

on behalf of the Verts/ALE Group

**Motion for a resolution
Paragraph 13**

Motion for a resolution

13. *Notes that* the Strategic Compass *will* enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into *capability needs*, including in cyber defence, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

Amendment

13. *Underlines the need for the HR/VP and the Member States to use* the Strategic Compass *process to* enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into *better common and national capabilities*, including in *military* cyber defence, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

Or. en

Amendment 131
Petras Auštrevičius

Motion for a resolution
Paragraph 13

Motion for a resolution

13. Notes that the Strategic Compass will enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into capability needs, including in cyber defence, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

Amendment

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

Or. en

Amendment 132
Tom Vandenkendelaere

Motion for a resolution

Paragraph 13

Motion for a resolution

13. Notes that the Strategic Compass will enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into capability needs, including in cyber defence, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

Amendment

13. Notes that the Strategic Compass will enhance and guide the implementation of the EU's level of ambition in security and defence, and translate that ambition into capability needs, including in cyber defence **as a priority item**, thereby increasing the ability of the EU and Member States to prevent, discourage, deter, respond to and recover from malicious cyber activities by strengthening its posture, situational awareness, tools, procedures and partnerships;

Or. en

Amendment 133

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 13 a (new)

Motion for a resolution

Amendment

13 a. Calls on all Member States to ensure coherence and focus on cyber capability, developing a strategic common approach to priorities; calls on fostering research, innovation and the exchange of expertise, in order to guarantee the full potential of PESCO and EDF;

Or. en

Amendment 134

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution

Paragraph 14

Motion for a resolution

Amendment

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

14. Insists that the Strategic Compass should deepen the strategic culture in the cyber domain and remove any duplication of capabilities and mandates; stresses that it is essential to overcome the current fragmentation and complexity of the overall cyber architecture within the EU **and to develop a common vision on how to achieve security and stability in cyberspace;**

Or. en

Amendment 135

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 14

Motion for a resolution

Amendment

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

14. Insists that the Strategic Compass, should **contribute to creating a common** 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;

Or. en

Amendment 136

Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

Motion for a resolution

Paragraph 14

Motion for a resolution

Amendment

14. Insists that **the Strategic Compass should deepen the strategic culture in the cyber domain and remove any duplication**

14. Insists that, **when it comes digital technology and cyber security in particular, each State has the right to**

of capabilities and mandates; stresses that it is essential to overcome the current fragmentation and complexity of the overall cyber architecture within the EU;

possess its own language and codes, which the European Union institutions cannot under any circumstances oblige them to disclose;

Or. fr

Amendment 137

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 14 a (new)

Motion for a resolution

Amendment

14 a. Recalls the importance of the EU cyber deterrence stance and the related issue of attribution to cyber-attacks as one of the key tools for strengthening EU and Member States' capabilities to deter and respond to malicious behavior in cyberspace; calls on the Council to use the EU's cyber diplomacy toolbox, including restrictive measures, more often and in a coherent way; invites to consider joint public attribution of malicious cyber activities, including the option to create cyber-behavior reports under the auspices of the EEAS for specific actors to summarize state sponsored malicious cyber activities against Member States at EU-level; underlines the need to strengthen the European Union Intelligence and Situation Centre (EU INTCEN) capabilities to analyse and assess Member States information and intelligence on malicious cyber activities and incidents;

Or. en

Amendment 138
Assita Kanko

Motion for a resolution
Paragraph 14 a (new)

Motion for a resolution

Amendment

14 a. Underlines that the European Union could take further action in the cyber security challenges and address new cyber defence capabilities if starts a cooperation with third countries or third partners;

Or. en

Amendment 139
Assita Kanko

Motion for a resolution
Paragraph 14 b (new)

Motion for a resolution

Amendment

14 b. Considers that Member States should consider isolating part of their 2%-20% defence spending obligations to include a dedicated minimum expenditure towards research and development within their defence budgets;

Or. en

Amendment 140
Assita Kanko

Motion for a resolution
Paragraph 14 c (new)

Motion for a resolution

Amendment

14 c. Strongly encourages the foundation of an Advisory Group for Small and Medium Enterprises (SME) to the EDA to advise EU on how to keep pace with technological change; A key objective for these efforts should be to encourage the development of an AI-

focused agenda for R&D within Member States;

Or. en

Amendment 141

Assita Kanko

Motion for a resolution

Paragraph 14 d (new)

Motion for a resolution

Amendment

14 d. Recommends Member States and EU's various defence agencies implement, as a matter of urgency, the prioritization of developments in new technologies, specifically AI, machine learning, military application of nano and bio-technologies and developing counter weights to the threats posed by CBRN weapons and new missile technologies;

Or. en

Amendment 142

Assita Kanko

Motion for a resolution

Paragraph 14 e (new)

Motion for a resolution

Amendment

14 e. Recommends the establishment of a Current Assets Framework be established that would purposively focus on the more efficient use of existing assets and capabilities;

Or. en

Amendment 143

Assita Kanko

Motion for a resolution
Paragraph 14 f (new)

Motion for a resolution

Amendment

14 f. Establish a Future Requirements Framework that identified the operational capabilities that Member States need and how best to obtain them by 2030;

Or. en

Amendment 144
Assita Kanko

Motion for a resolution
Paragraph 14 g (new)

Motion for a resolution

Amendment

14 g. Highlights the role AI can play in providing advanced training and pre-deployment unit-level preparation for EU or NATO-led forces during peacetime to ensure a rapid yet smooth transition into conducting operations;

Or. en

Amendment 145
Assita Kanko

Motion for a resolution
Paragraph 14 h (new)

Motion for a resolution

Amendment

14 h. Encourages developing a set of common EU AI capabilities matched to a Member State's operating concepts to bridge technical gaps to 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;

Amendment 146**Markéta Gregorová**

on behalf of the Verts/ALE Group

Motion for a resolution**Paragraph 15***Motion for a resolution*

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

Amendment

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at **national and** EU level, **both in terms of quantity and quality**; urges the VP/HR and/or the Member States to increase financial and personnel resources, **and their training**, in particular experts in cyberforensics **because the individuals and organisations behind many cyber attacks cannot be identified within short time frames, which causes majors problems as regards the organisation of adequate political, civilian and military responses**; calls for further funding for CERT-EU and the creation of an EU security operations centre;

Amendment 147**Urmas Paet, Christophe Grudler, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans****Motion for a resolution****Paragraph 15***Motion for a resolution*

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

Amendment

15. Stresses that fragmentation is accompanied by serious concerns over **the lack of** resources and staff at the EU level, **thereby stresses the need to increase both**; urges the VP/HR and/or the Member States to increase financial and **cyber defence** personnel resources **in decision and policy**

the creation of an EU security operations centre;

making, policy implementation, cyber incidents response and investigation areas, including the development of cyber skills; calls for further funding for CERT-EU and the creation of an EU security operations centre;

Or. en

Amendment 148
Petras Auštrevičius

Motion for a resolution
Paragraph 15

Motion for a resolution

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

Amendment

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at the EU level; ***notes that the EU lags far behind the US in investing in cyber-defence, which hinders the ambition of creating the most secure digital environment***; urges the VP/HR and/or the Member States to increase financial and personnel resources, in particular experts in cyberforensics; calls for further funding for CERT-EU and the creation of an EU security operations centre;

Or. en

Amendment 149
Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution
Paragraph 15

Motion for a resolution

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at the EU level; urges the VP/HR and/or the Member States to

Amendment

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at the EU level; urges the VP/HR and/or the Member States to

increase financial and personnel resources, in particular experts in cyberforensics; calls for further funding for CERT-EU and the creation of an EU security operations centre;

increase financial and personnel resources, in particular experts in cyberforensics **to strengthen EU's ability to characterize, attribute cyber attacks and hence provide the adequate response**; calls for further funding for CERT-EU and the creation of an EU security operations centre;

Or. en

Amendment 150

Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution

Paragraph 15

Motion for a resolution

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

Amendment

15. Stresses that fragmentation is accompanied by serious concerns over resources and staff at the EU level; urges the VP/HR and/or the Member States to **significantly** increase financial and personnel resources, in particular experts in cyberforensics; calls for further funding for CERT-EU and **support Member States in establishing and strengthening Security Operation Centres (SOCs) in order to build a network of SOC's across the EU**;

Or. en

Amendment 151

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 15

Motion for a resolution

15. Stresses that fragmentation is accompanied by **serious concerns over resources and staff at the EU level; urges the VP/HR and/or the Member States to**

Amendment

15. Stresses that fragmentation is accompanied by **the need** to increase financial and personnel resources, in particular **cyber intelligence analysts and**

increase financial and personnel resources, in particular experts in *cyberforensics*; calls for further funding for CERT-EU and *the creation of an EU security operations centre*;

experts in *cyber forensics*; calls for further funding for CERT-EU and *to support Member States in establishing and strengthening Security Operation Centres (SOCs) in order to build a network of SOCs across the EU*;

Or. en

Amendment 152
Nicolae Ștefănuță

Motion for a resolution
Paragraph 15

Motion for a resolution

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

Amendment

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

Or. en

Amendment 153
David McAllister

Motion for a resolution
Paragraph 15

Motion for a resolution

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

Amendment

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

Amendment 154
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 15 a (new)

Motion for a resolution

Amendment

15 a. Notes the important training work undertaken by the European Security and Defence College in the cyber defence field, and welcomes in this respect the establishment of the Cyber Education, Training, Evaluation and Exercise (ETEE) Platform, aiming at addressing cyber security and defence training among the civilian and military personnel as well as establishing the necessary harmonization and standardization in cyber related training; stresses that ESDC should benefit from structural Union funding to be able to enhance its contribution to foster the EU cyber defence skills, especially given the increased need for top level cyber experts;

Or. en

Amendment 155
Arnaud Danjean

Motion for a resolution
Paragraph 15 a (new)

Motion for a resolution

Amendment

15a. Calls for measures to strengthen operational cooperation between Member States, particularly in the event of cyber security crises and incidents;

Or. fr

Amendment 156
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 15 b (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 157
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 16

Motion for a resolution

Amendment

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

16. Recalls that cyber defence has both military and civilian dimensions; **stresses the need to first analyse and discuss problems of cooperation, coordination, but also gaps as regards human and technical resources both at national and EU level**; calls on the VP/HR, therefore, to develop an integrated policy approach and close cooperation between the Military CERT-Network and CERT-EU;

Or. en

Amendment 158
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 16

Motion for a resolution

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

Amendment

16. Recalls that cyber defence **requires strong** military and civilian **cooperation, synergies and coherence of instruments**; **therefore** calls on the **EU Commission** to develop an integrated policy approach and close cooperation between the **Computer Security Incident Response Teams CSIRTs Network and the foreseen** Military CERT-Network;

Or. en

Amendment 159

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 16

Motion for a resolution

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

Amendment

16. Recalls that cyber defence has both military and civilian dimensions; calls on the VP/HR, therefore, to develop an integrated policy approach and close cooperation between the **Computer Security Incident Response Teams CSIRTs Network and the foreseen** Military CERT-Network;

Or. en

Amendment 160

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Recalls that cyber defence has both military and civilian dimensions; calls on

Amendment

16. Recalls that cyber defence has both military and civilian dimensions; calls on

the VP/HR, therefore, to develop an integrated policy approach and **close cooperation** between the Military CERT-Network and **CERT-EU**;

the VP/HR, therefore, to develop an integrated policy approach and **promote synergies** between the Military CERT-Network and **the CSIRTs Network**;

Or. en

Amendment 161

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution **Paragraph 16 a (new)**

Motion for a resolution

Amendment

16 a. 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 the NATO's Locked Shields exercise, as one of the best examples of testing and improving Cyber Defence Capability, both civilian and military;

Or. en

Amendment 162

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution **Paragraph 16 a (new)**

Motion for a resolution

Amendment

16 a. Stresses that cyber defence capabilities are crucial for ensuring secure and resilient information exchange and protection between intelligence EU and MS entities and SatCen in both security from space (GEOINT) and in space (SST) in order to preserve and enhance the required strategic autonomy on situational awareness at EU level.

Amendment 163
Petras Auštrevičius

Motion for a resolution
Paragraph 16 a (new)

Motion for a resolution

Amendment

16 a. Stresses the importance of strengthening cyber security governance, in particular the planning process, in order to increase public-private partnerships;

Or. en

Amendment 164
Emmanuel Maurel

Motion for a resolution
Paragraph 16 a (new)

Motion for a resolution

Amendment

16a. Is concerned about the European Union's dependence on the digital platforms of foreign powers, particularly the US, when it comes to ensuring its cyber security;

Or. fr

Amendment 165
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 16 b (new)

Motion for a resolution

Amendment

16 b. Stresses the importance of education to raise public awareness and to improve the skills of citizens to defend themselves against cybercriminal activity and cyberattacks;

Or. en

Amendment 166
Petras Auštrevičius

Motion for a resolution
Paragraph 16 b (new)

Motion for a resolution

Amendment

16 b. Calls for public awareness of cyber security threats and a focus on cyber defence in education, training and exercises;

Or. en

Amendment 167
Juozas Olekas

Motion for a resolution
Paragraph 17

Motion for a resolution

Amendment

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

17. **Takes note of** 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 EU’s digital leadership and its strategic capacities**;

Or. en

Amendment 168
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 17

Motion for a resolution

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

Amendment

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

Or. en

Amendment 169
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 17 a (new)

Motion for a resolution

17 a. Promotes 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 the European competitiveness in the cybersecurity market and boosting the internal demand;

Amendment

Or. en

Amendment 170

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 17 a (new)

Motion for a resolution

Amendment

17 a. Notes the important role the Joint Cyber Unit will play in protecting the EU from grave cross-border cyber-attacks, based on the concept of cross-sector information-sharing; underlines the importance of coordination in order to avoid the duplication of structures and responsibilities during the development;

Or. en

Amendment 171

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Paragraph 17 a (new)

Motion for a resolution

Amendment

17 a. Welcomes the Commission's initiative to build a network of Security Operations Centres across the EU which could enhance civil-military cooperation to provide timely warnings on cybersecurity incidents;

Or. en

Amendment 172

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 17 b (new)

Motion for a resolution

Amendment

17 b. Urges the Commission and the Member states to establish without delay Member States' EU cyber intelligence working group within the EU intelligence and Situation Centre (INTCEN) to advance strategic intelligence cooperation on cyber threats and activities, as foreseen in "The EU's Cybersecurity Strategy for the Digital Decade";

Or. en

Amendment 173

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 17 c (new)

Motion for a resolution

Amendment

17 c. Underlines the important role the new Cybersecurity Competence Centre in Bucharest will play and calls for its concrete role and competences to be identified as soon as possible;

Or. en

Amendment 174

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 18

Motion for a resolution

Amendment

18. Recalls that improving cyber defence capabilities also requires civilian network and information security expertise; welcomes the proposed revision

18. Recalls that improving cyber defence capabilities also requires civilian network and information security expertise; welcomes the proposed revision

of the Directive on security of network and information systems (NIS) and of current EU law, seeking to protect critical infrastructures, enhance supply chain security and the inclusion of regulated actors in the digital ecosystem;

of the Directive on security of network and information systems (NIS) and of current EU law, seeking to protect critical infrastructures, enhance supply chain security and the inclusion of regulated actors in the digital ecosystem; ***recalls that, on a national level, each EU Member State should have a dedicated policy towards cybersecurity supply chain risk management addressing, in particular, the question of trusted vendors; recalls that on EU level, existing platforms such as NIS Cooperation Group could be used to carry out coordinated security risk assessments of specific critical ICT services, systems or products supply chains, building on successful cooperation between the Member States on establishing 5G toolbox;***

Or. en

Amendment 175

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler

Motion for a resolution

Paragraph 18

Motion for a resolution

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

Amendment

18. Recalls that improving cyber defence capabilities also requires civilian network and information security expertise; welcomes the proposed revision of the Directive on security of network and information systems (NIS) and of current EU law, seeking to protect critical infrastructures, enhance supply chain security and the inclusion of regulated actors in the digital ecosystem; ***recalls that the NIS Directive should respect Member States competencies, in particular their responsibility regarding national security;***

Or. en

Amendment 176
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 18

Motion for a resolution

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

Amendment

18. Recalls that improving cyber defence capabilities also requires, ***given their often dual-use nature***, civilian network and information security expertise; ***notes the importance of promoting civil-military cooperation***; welcomes the proposed revision of the Directive on security of network and information systems (NIS) and of current EU law, seeking to protect critical infrastructures, enhance supply chain security and the inclusion of regulated actors in the digital ecosystem;

Or. en

Amendment 177
Markéta Gregorová
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 18

Motion for a resolution

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

Amendment

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

Or. en

Amendment 178
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 18 a (new)

Motion for a resolution

Amendment

18 a. Underlines that cooperation with the private sector and civilian stakeholders, including industries and entities involved in the management of critical infrastructures, is crucial and should be reinforced due to the intrinsic characteristics of the cyber domain, in which technological innovation is mainly driven by private companies that often do not operate in the military field;

Or. en

Amendment 179
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 18 a (new)

Motion for a resolution

Amendment

18 a. 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;

Or. en

Amendment 180
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 18 b (new)

Motion for a resolution

Amendment

18 b. Promotes a common vision on Cloud adoption strategy for sensitive sectors with the aim of defining a European approach based on shared standards among like-minded States, in order to protect the digital know-how, sensitive data and information;

Or. en

Amendment 181
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 19

Motion for a resolution

Amendment

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

19. Welcomes the Commission's Action Plan on Synergies between civil, defence and space industries and recalls the close interdependence of these three sectors **for** cyber defence; notes that, differently from other military domains, cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological dependencies on third parties; **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, stresses that EU SatCen should benefit from structural Union funding to be able to maintain its contributions to the Union's actions; underlines the need for the EU to strive to prevent the weaponization of space;** strongly believes that the EU needs to increase its technological sovereignty and innovation, **supporting research and technology** investing in the **ethical** use of new technologies **insecurity** and defence

like Artificial Intelligence (AI) and quantum computing; ***stresses however that the military use of AI must respect international Human Rights law and international humanitarian law, and that the EU shall take the lead in promoting a global AI regulatory framework rooted in democratic values and a human-in-the-loop approach;***

Or. en

Amendment 182

Jérôme Rivière, Thierry Mariani, Jaak Madison, Harald Vilimsky

Motion for a resolution

Paragraph 19

Motion for a resolution

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

Amendment

19. Welcomes the Commission's Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological dependencies on third parties; strongly believes that the EU needs to increase its technological sovereignty and innovation, investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing; ***affirms that data protection is a legal must, particularly when it comes to defending not only the vital interests of the State but also individual freedom and security;***

Or. fr

Amendment 183

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group

Rasa Juknevičienė

Motion for a resolution
Paragraph 19

Motion for a resolution

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

Amendment

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

Or. en

Amendment 184
David McAllister

Motion for a resolution
Paragraph 19

Motion for a resolution

19. Welcomes the Commission's Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological dependencies on third

Amendment

19. Welcomes the Commission's Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, *the infrastructure used to "create"* cyber space is mainly owned by commercial entities based mostly outside the EU, which leads to industrial and technological

parties; strongly believes that the EU needs to increase its technological sovereignty and innovation, investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing;

dependencies on third parties; strongly believes that the EU needs to increase its technological sovereignty and innovation, **and additionally** investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing;

Or. en

Amendment 185

David Lega

Motion for a resolution

Paragraph 19

Motion for a resolution

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

Amendment

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

Or. en

Amendment 186

Antonio López-Istúriz White

Motion for a resolution

Paragraph 19

Motion for a resolution

19. Welcomes the Commission's

Amendment

19. Welcomes the Commission's

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

Action Plan On Synergies between civil, defence and space industries, and recalls the close interdependence of these three sectors in cyber defence; notes that, differently from other military domains, cyber space is mainly *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 innovation, investing in the use of new technologies in security and defence such as artificial intelligence (AI) and quantum computing;

Or. en

Amendment 187
Traian Băsescu

Motion for a resolution
Paragraph 19 a (new)

Motion for a resolution

Amendment

19a. Welcomes the political agreement between the European Parliament and the Council on the Regulation establishing the European Cybersecurity Industrial, Technology and Research Competence Centre with a network of national coordination centres; stresses the importance of the Centre in implementing relevant cybersecurity projects and initiatives that will help create the new capacities essential to underpin Union resilience and step up coordination between the civilian and defence cybersecurity sectors when it comes to defining their tasks and responsibilities;

Or. ro

Amendment 188
Tom Vandenkendelaere

Motion for a resolution
Paragraph 19 a (new)

Motion for a resolution

Amendment

19 a. *Stresses the need to counter cyber attacks of countries whose aggression has been experienced more than once in the past by the EU and its Member States; recognizes that cyber defence is neither efficient nor effective as long as it does not contain offensive means and measures as well; underlines that explicit attribution of cyber attacks is a useful instrument of deterrence, while recognizing the need for prudence from the political and diplomatic point of view; recommends to take the option of attributing cyber attacks on the basis of credible evidence at least into consideration;*

Or. en

Amendment 189

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution
Paragraph 19 a (new)

Motion for a resolution

Amendment

19 a. *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 as well as non-state adversaries; calls on the Commission and Member States to activate several levers, such as certification as well as the supervision of the responsibility of private actors;*

Or. en

Amendment 190

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 19 b (new)

Motion for a resolution

Amendment

19 b. Recommends that the establishment of a Joint Cyber Unit to increase cooperation to respond to the lack of information sharing among EU institutions, bodies and agencies guaranteeing a secure and rapid information network and to enable the full use of existing structures, resources and capabilities;

Or. en

Amendment 191

Nicolae Ștefănuță

Motion for a resolution

Paragraph 20

Motion for a resolution

Amendment

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

20. Welcomes the upcoming ‘Military Vision and Strategy on Cyberspace as a Domain of Operations’ which will define cyberspace as a domain of operations for EU CSDP; calls for continuous assessment of the vulnerabilities of **the information infrastructures 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;

Or. en

Amendment 192

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart

Groothuis

**Motion for a resolution
Paragraph 20 a (new)**

Motion for a resolution

Amendment

20 a. Deplores that currently the EU Military Planning and Conduct Capability (MPCC) has limitations in the classified systems that are hampering its capabilities; calls therefore on the EEAS to swiftly provide the MPCC with a state-of-the-art autonomous and secure Communications and Information System (CIS) able to handle up to “EU Secret” data for its CSDP missions and operations and with a level of protection and resilience that is adequate with a deployed FHQ;

Or. en

**Amendment 193
Fabio Massimo Castaldo**

**Motion for a resolution
Paragraph 20 a (new)**

Motion for a resolution

Amendment

20 a. Calls on the Member State, to adopt policies able to ensure the widest possible access to the most performing cyber security tools, supporting companies, SMEs and businesses with low financial capabilities, through benefits, grants, loans or fiscal advantages dedicated to the acquisition of highest level cybersecurity products and services, avoiding that their costs represent an element of discrimination;

Or. en

Amendment 194

Assita Kanko

**Motion for a resolution
Paragraph 20 a (new)**

Motion for a resolution

Amendment

20 a. Notes the growing importance of space security and satellites, stresses the importance of the European Union Satellite Centre and requests the agency to analyse and provide a report regarding the safety and/or vulnerabilities of the EU and Member States satellites to space debris, cyber attack and direct missile attack;

Or. en

Amendment 195

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

**Motion for a resolution
Paragraph 20 a (new)**

Motion for a resolution

Amendment

20 a. Notes that a streamlined EU military training & education in the cyber domain would significantly improve the level of trust among Member States, increasing standard operating procedures and clearer regulations and enforcement;

Or. en

Amendment 196

Fabio Massimo Castaldo

**Motion for a resolution
Paragraph 20 b (new)**

Motion for a resolution

Amendment

20 b. Calls on Member States to promote

partnerships with Academia aimed at fostering R&D cybersecurity programme in order to develop new common technologies, tools and skills applicable in both civilian and defence sectors through a multidisciplinary approach. Partnerships should be financed by existing and new funding tools under the auspices of the European Commission;

Or. en

Amendment 197

David Lega

Motion for a resolution Paragraph 21

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Amendment

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States; ***expresses its embarrassment and serious concerns about the security of confidential EU meetings, as a Dutch journalist managed to access a confidential videoconference at the level of EU defence ministers last year. Underlines that such weaknesses in the EU institutions security practices have***

adverse effects on the credibility of EU cyber defence capabilities;

Or. en

Amendment 198

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution Paragraph 21

Motion for a resolution

21. Calls for enhanced mutual **operational** assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a **hypothetical** cyber attack scenario; **calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE)**; calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Amendment

21. Calls **to further integrate cybersecurity into EU crisis response mechanisms and link the existing initiatives, structures and procedures (such as the IPCR, the CSIRTs Network, the NIS Cooperation Group, the CyCLONE) between various cyber communities** for enhanced mutual assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the **stake of solidarity and mutual assistance clause** (Article 42(7) of the TEU) in a cyber attack scenario; calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States; **welcomes further discussions on the articulation between the EU cybersecurity crisis management framework and the cyber diplomacy toolbox;**

Or. en

Amendment 199

Emmanuel Maurel

**Motion for a resolution
Paragraph 21**

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for ***increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE)***; calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Amendment

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Or. fr

Amendment 200

Henna Virkkunen

on behalf of the PPE Group

Rasa Juknevičienė

**Motion for a resolution
Paragraph 21**

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of ***further*** exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a

Amendment

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of ***joint*** exercises and scenario-based policy discussions on crisis management ***between Member States to increase interoperability and develop a common***

hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and **Article 222** of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

understanding of cyber defence, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical ***grave*** cyber attack scenario ***that amounts to a use of force or an armed attack***; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and **Article 222** of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Or. en

Amendment 201

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 21

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific

Amendment

21. Calls for enhanced mutual operational assistance between Member States ***in particular in the event of major cyber attacks such as the one on Estonia in 2007***; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or

objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Or. en

Amendment 202
Petras Auštrevičius

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Amendment

21. Calls for enhanced mutual operational assistance between Member States; 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) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on the EU institutions or Member States;

Or. en

Amendment 203
Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj

Motion for a resolution

Paragraph 21

Motion for a resolution

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on *the EU institutions or* Member States;

Amendment

21. Calls for enhanced mutual operational assistance between Member States; strongly emphasises the importance of further exercises and scenario-based policy discussions on crisis management, including on the mutual assistance clause (Article 42(7) of the TEU) in a hypothetical cyber attack scenario; calls for increased coordination with NATO in this matter through participation in cyber exercises and joint training, such as the parallel and coordinated exercises (PACE); calls for such initiatives to strengthen the common understanding on the implementation procedures for mutual assistance and/or solidarity in line with Article 42(7) of the TEU and Article 222 of the TFEU, including with a specific objective of operationalising these procedures for cyber-attacks on *EU* Member States;

Or. en

Amendment 204

Bart Groothuis, Nathalie Loiseau, Klemen Grošelj, Javier Nart

Motion for a resolution

Paragraph 21 a (new)

Motion for a resolution

Amendment

21 a. 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 itself often not serious enough to trigger Article 5 of the NATO treaty or Article 42(7) of the TEU,

though have a strategic effect cumulative and cannot be effectively tackled by 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 a way that would reserve the right for collective defence below the collective defence threshold and allow for collective countermeasures of EU Member States on a voluntary basis, and work internationally with allies for a similar solution at the international level; Underlines that this is the only effective means to counter the paralysis in reacting against hybrid threats and an instrument to increase the costs for our adversaries;

Or. en

Amendment 205

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution Paragraph 21 a (new)

Motion for a resolution

Amendment

21 a. Reiterates that common strong attribution capabilities are also an essential component of effective cyber defence and cyber deterrence; welcomes the VP/HR proposal to encourage and facilitate the establishment of a Member States' EU cyber intelligence working group residing within the EU Intelligence and Situation Centre (INTCEN) to advance strategic intelligence cooperation on cyber threats and activities, in order to further support EU situational awareness and decision-making on a joint diplomatic response;

Or. en

Amendment 206
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 21 a (new)

Motion for a resolution

Amendment

21 a. Welcomes the adoption, based on Article 48 (2) of the Cybersecurity Act, of a cybersecurity certification scheme that will serve as a successor to the SOG-IS Mutual Recognition Agreement and of further certification schemes and standards for specific technologies;

Or. en

Amendment 207
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 21 b (new)

Motion for a resolution

Amendment

21 b. Considers that Cybersecurity is not only a technology problem; Calls for the adoption, based on Articles 7 and 8 of the Cybersecurity Act, of an enhanced awareness program that improves ‘cyber-hygiene’ in citizens, organizations and businesses against Cyber Threats and Disinformation;

Or. en

Amendment 208
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 22

Motion for a resolution

Amendment

22. Considers **that** EU-NATO cyber

22. Considers **the** EU-NATO cyber

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

cooperation crucial, *which could enable and strengthen* formal *collective* attribution *of cyber malicious incidents and consequently* the imposition of restrictive sanctions *and measures*; notes that *effective cyber* deterrence would be achieved if *perpetrators are* aware of the catalogue of countermeasures (based on *severity/scale/target* of the *cyber attacks*); *calls on Member States to fully share evidence and intelligence in order to feed into the establishment of cyber sanction lists*;

Or. en

Amendment 209

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution Paragraph 22

Motion for a resolution

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

Amendment

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

Or. en

Amendment 210 Arnaud Danjean

Motion for a resolution Paragraph 22

Motion for a resolution

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

Amendment

22. Considers that cyber **defence** cooperation with NATO plays an important role in preventing, deterring and responding to cyber attacks affecting Member States' collective security;

Or. fr

Amendment 211

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 22

Motion for a resolution

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

Amendment

22. Considers that EU-NATO cyber cooperation is crucial, as it enables strong formal attribution and thus the imposition of restrictive sanctions; notes that **in general**, functioning deterrence would be achieved if adversaries were aware of the catalogue of possible **credible** countermeasures, **and their proportionality and appropriateness, their compliance with international law, in particular the UN Charter** (based on the severity, scale, and target of the cyber-attacks);

Or. en

Amendment 212

Antonio López-Istúriz White

Motion for a resolution

Paragraph 22

Motion for a resolution

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

Amendment

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

Or. en

Amendment 213
Emmanuel Maurel

Motion for a resolution
Paragraph 22

Motion for a resolution

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

Amendment

22. Considers that cyber cooperation ***between Member States is crucial***; notes that functioning deterrence would be achieved if adversaries were aware of the catalogue of possible countermeasures (based on the severity, scale, and target of the cyber-attacks);

Or. fr

Amendment 214
Jérôme Rivière, Thierry Mariani

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Considers that EU-NATO cyber cooperation ***is crucial, as it enables strong***

Amendment

22. Considers that EU-NATO cyber cooperation ***should not form the basis of***

formal attribution and thus the imposition of restrictive sanctions; notes that functioning deterrence would be achieved if adversaries were aware of the catalogue of possible countermeasures (based on the severity, scale, and target of the cyber-attacks);

measures to combat cyber crime; warns of the risks of data transfers taking place solely for the benefit of the US and undermining the principles of personal data privacy;

Or. fr

Amendment 215

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution **Paragraph 22**

Motion for a resolution

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

Amendment

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

Or. en

Amendment 216

David McAllister

Motion for a resolution **Paragraph 22**

Motion for a resolution

22. Considers that EU-NATO cyber cooperation is crucial, as it enables strong formal attribution and thus the imposition of restrictive sanctions; notes that functioning **deterrence** would be achieved if adversaries were aware of the catalogue

Amendment

22. Considers that EU-NATO cyber cooperation is crucial, as it enables strong formal attribution and thus the imposition of restrictive sanctions; notes that functioning **resilience** would be achieved if adversaries were aware of the catalogue of

of possible countermeasures (based on the severity, scale, and target of the cyber-attacks);

possible countermeasures (based on the severity, scale, and target of the cyber-attacks);

Or. en

Amendment 217

Assita Kanko

Motion for a resolution

Paragraph 22 a (new)

Motion for a resolution

Amendment

22 a. Recognises that EU & NATO should coordinate on issue's where China's actions are contrary to Euro-Atlantic security interests; prioritization should be given to challenges in the cyber, hybrid, EDT, space, arms control, and non-proliferation areas;

Or. en

Amendment 218

Assita Kanko

Motion for a resolution

Paragraph 22 b (new)

Motion for a resolution

Amendment

22 b. Recognises that China's acquisitions of intellectual property and technological advances by leading research centres are often used to propel its military aims and therefore the EU should work to develop a long-term strategy to counter China's military-civil fusion (MCF) strategy in Europe;

Or. en

Amendment 219

Assita Kanko

**Motion for a resolution
Paragraph 22 c (new)**

Motion for a resolution

Amendment

22 c. Calls on EDA to ensure that any efforts it takes to enhance Member States operational capabilities take place in close conjunction with NATO's Defence Investment Division and the NATO support and Procurement Agency;

Or. en

Amendment 220

Assita Kanko

**Motion for a resolution
Paragraph 22 d (new)**

Motion for a resolution

Amendment

22 d. Urges EU-NATO cooperation in regulating 5G implementation to comply with strict national security standards that secures national and international information networks capable of encrypting communications;

Or. en

Amendment 221

Assita Kanko

**Motion for a resolution
Paragraph 22 e (new)**

Motion for a resolution

Amendment

22 e. Encourages further progress in the common set of proposals, particularly the ongoing interaction with the new EU Hybrid Fusion Cell and NATO's Hybrid Analysis Cell in sharing situational

awareness and analysis, tactical and operational cooperation between Operation Sea Guardian and EUNAVFOR MED Sophia and ongoing cooperation between EU's Computer Emergency Response Team and the NATO Computer Incident Response Capability;

Or. en

Amendment 222
Emmanuel Maurel

Motion for a resolution
Paragraph 23

Motion for a resolution

Amendment

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

deleted

Or. fr

Amendment 223
Nicolae Ștefănuță

Motion for a resolution
Paragraph 23

Motion for a resolution

Amendment

23. Welcomes the arrangement between the CERT-EU and the NATO Computer Incident Response Capability (NCIRC), to ensure the ability to respond

23. Welcomes the arrangement between the CERT-EU and the NATO Computer Incident Response Capability (NCIRC), to ensure the ability to respond

to threats in real time; stresses also the importance to increase cyber defence training capabilities in IT and cyber systems in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and the NATO Communications and Information (NCI) Academy;

to threats in real time ***by improving cyber incident prevention, detection and response both in the EU and in NATO***; stresses also the importance to increase cyber defence training capabilities in IT and cyber systems in cooperation with the NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) and the NATO Communications and Information (NCI) Academy;

Or. en

Amendment 224
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 23 a (new)

Motion for a resolution

Amendment

23 a. Calls on all Member State and EU, to provide themselves with a Cyber Deterrence Set of Forces, able to provide NATO of a coordinated, efficient and performing instrument of counter-cyber-attack, even updating the juridical framework in a way that will consider the cyber deterrence as an acceptable and proportionate reaction option to respond to attacks, prevent the recurrence and disable potential hostile forces in presence of a concrete threat for security of people, enterprises, human rights, free institutions and democracy;

Or. en

Amendment 225
Assita Kanko

Motion for a resolution
Paragraph 23 a (new)

Motion for a resolution

Amendment

23 a. Recognises the emerging threat of Hyper war and the unique requirements this will place on defence architectures and the need for a high-tech industrial base if the EU and NATO are to preserve an adequate deterrence and defence posture or simply maintain a comparative advantage against adversarial actors;

Or. en

Amendment 226
Assita Kanko

Motion for a resolution
Paragraph 23 b (new)

Motion for a resolution

Amendment

23 b. Stresses concern regarding the 2018 Russian Ministry of Defence's ten-point plan to place AI at the core of Russian military modernization, driven by AI consortia across government, industry and academia; Recognises that this is bolstered by the creation of a Fund for Analytical Algorithms combined with a state system for training and educating AI specialists;

Or. en

Amendment 227
Assita Kanko

Motion for a resolution
Paragraph 23 c (new)

Motion for a resolution

Amendment

23 c. Stresses the concern posed by Russia's harmonisation of highly disruptive propaganda and kinetic operations while committing to investments in military-relevant AI;

Amendment 228

Assita Kanko

Motion for a resolution

Paragraph 23 d (new)

Motion for a resolution

Amendment

23 d. Recognises the synergy between old and new military technologies that will be utilized for hyper war such as combining aircraft, ships, submarines and tanks with intelligent drone swarms or hypersonic stand-off munitions;

Or. en

Amendment 229

Assita Kanko

Motion for a resolution

Paragraph 23 e (new)

Motion for a resolution

Amendment

23 e. Urges EDA, CDP, CARD and NDPP to utilize autonomous software to assist with maintenance, logistics management, and targeting of offensive and defensive systems to ensure that a CSDP force is successfully integrated with autonomous, unmanned ground, air and sea vehicles to provide a standardised, and ever increasing, level of operational competence and consistency of execution;

Or. en

Amendment 230

Assita Kanko

Motion for a resolution

Paragraph 23 f (new)

Motion for a resolution

Amendment

23 f. Urges the EU's PESCO and promotion of pooling and sharing, as well as NATO's Smart Defence, Connected Forces Initiative and Defence Investment Pledge be reinforced by an EU-NATO Capability Action Plan that seeks to better forge synergies, harmonization and efficiencies into the relationship between suppliers and end-users;

Or. en

Amendment 231

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 24

Motion for a resolution

Amendment

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

24. Calls for further synchronisation of EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities, avoiding duplication and acknowledging their respective responsibilities; **welcomes the progress made in the EU-NATO cooperation in the cyber defence field, notably on the exchanges of concepts and doctrines, on cross participation in cyber exercises and on cross-briefings notably on the cyber dimension of crisis managements;**

Or. en

Amendment 232

Urmas Paet, Nicolae Ștefănuță, Christophe Grudler, Michal Šimečka, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 24

Motion for a resolution

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

Amendment

24. Calls for further synchronisation of EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities, ***pursuing the affiliation of relevant CSDP structures to NATO's Federated Mission Networking and*** avoiding duplication and acknowledging their respective responsibilities;

Or. en

Amendment 233

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution

Paragraph 24

Motion for a resolution

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

Amendment

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

Or. en

Amendment 234

David McAllister

Motion for a resolution

Paragraph 24

Motion for a resolution

24. Calls for further ***synchronisation of*** EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities,

Amendment

24. Calls for further EU-NATO cooperation, notably on cyber defence interoperability requirements, by looking for possible complementarities, avoiding

avoiding duplication and acknowledging their respective responsibilities;

duplication and acknowledging their respective responsibilities;

Or. en

Amendment 235
Tom Vandenkendelaere

Motion for a resolution
Paragraph 24 a (new)

Motion for a resolution

Amendment

24 a. Emphasises that both the EU and NATO should further strengthen their capabilities to prevent, deter and respond to hybrid and cyber attacks; suggests the creation of a joint cyber threat information hub, as well as a joint task force for cyber security; emphasises the relevance of a common EU/NATO cyber threat analysis on the basis of which important and less important, urgent and less urgent decisions should be taken and actions could be selected and launched;

Or. en

Amendment 236
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 24 a (new)

Motion for a resolution

Amendment

24 a. Underlines the important 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;

Or. en

Amendment 237

Urmas Paet

Motion for a resolution

Paragraph 24 a (new)

Motion for a resolution

Amendment

24 a. Calls for increased cooperation and exchange of information with those that have increasingly been targeted by cyber attacks, such as Taiwan;

Or. en

Amendment 238

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 24 b (new)

Motion for a resolution

Amendment

24 b. Encourages the further promotion of the OSCE confidence-building measures for cyberspace;

Or. en

Amendment 239

Antonio López-Istúriz White

Motion for a resolution

Paragraph 25

Motion for a resolution

Amendment

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

25. **Acknowledges the fact that cyber threats are capable of compromising all traditional military domains, such as land, sea, air and space, traditional domains depend on cyber space functionality and not vice versa;** calls for closer coordination on cyber defence between Member States, the EU institutions, NATO, the United States and other strategic partners;

underlines the urgent need for implementing *a* widely-recognised international normative framework for responsible state behaviour in cyberspace;

Or. en

Amendment 240

Urmas Paet, Christophe Grudler, Nathalie Loiseau, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj, Hilde Vautmans

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

25. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO *Member States* and other strategic partners *like Japan, Australia, South Korea, New Zealand and others*; underlines 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 in cyberspace;

Or. en

Amendment 241

Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

25. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO, the United States and other strategic partners; underlines the urgent need *of states* for implementing the widely-recognised international normative

framework for responsible state behaviour in cyberspace;

framework for responsible state behaviour **and to contribute to the ongoing discussion on the modalities of application of international law** in cyberspace;

Or. en

Amendment 242

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

25. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO, the **UN, OSCE**, other strategic partners **and partnership countries, and for inclusive cooperation with civil society and stakeholders**; underlines the urgent need for implementing the widely-recognised international normative framework for responsible state behaviour in cyberspace;

Or. en

Amendment 243

Nicolae Ștefănuță

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

25. Calls for closer coordination on cyber defence between Member States, the EU institutions, NATO, the United States and other strategic partners **such as the Organisation for Security and Cooperation in Europe (OSCE)**; underlines the urgent need for implementing the widely-recognised international normative framework for

responsible state behaviour in cyberspace;

Or. en

Amendment 244

Markéta Gregorová

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

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

Or. en

Amendment 245

Emmanuel Maurel

Motion for a resolution

Paragraph 25

Motion for a resolution

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

Amendment

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

Or. fr

Amendment 246

Traian Băsescu

**Motion for a resolution
Paragraph 25 a (new)**

Motion for a resolution

Amendment

25a. Supports and encourages the enhancement of EU cybersecurity cooperation with candidate and potential candidate countries in the Western Balkans and with its eastern and southern neighbourhood partners as part of the Common Security and Defence Policy (CSDP); the development of security partnerships with the EU neighbourhood can facilitate the pooling of funding, knowledge, information and cyber capabilities in the region;

Or. ro

**Amendment 247
Fabio Massimo Castaldo**

**Motion for a resolution
Paragraph 25 a (new)**

Motion for a resolution

Amendment

25 a. 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 to re-launch a process aiming at concluding a formal and structured framework for cooperation in this field in the future;

Or. en

**Amendment 248
Juozas Olekas, Attila Ara-Kovács**

Motion for a resolution

Paragraph 26

Motion for a resolution

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

Amendment

26. ***Emphasizes the need to ensure peace and stability in the cyberspace***; calls on all Member States and the EU to show leadership during discussions and initiatives under the auspices of the *United Nations (UN)* to help truly *advance accountability, adherence to emerging norms, prevention of the misuse of digital technologies and* responsible state behaviour in *cyberspace* building on the consensus reports of the UN *Group of Governmental Experts* endorsed by the UN General Assembly; ***encourages the UN to foster dialogue among States, researchers, academics, civil society organisations, humanitarian actors and the private sector so as to have inclusive policymaking processes on 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 global negotiations to put in place an AI arms control regime***; calls for UN peacekeeping missions to be reinforced with cyber defence capacities in line with the effective implementation of their mandates;

Or. en

Amendment 249

Nathalie Loiseau, Petras Auštrevičius, Klemen Grošelj, Christophe Grudler, Bart Groothuis

Motion for a resolution

Paragraph 26

Motion for a resolution

26. Calls on all Member States and the EU to show leadership during discussions and initiatives under the auspices of the

Amendment

26. Calls on all Member States and the EU to show leadership during discussions and initiatives under the auspices of the

UN to help truly promote responsible state behaviour in cyber space, building on the consensus reports of the UN GGE endorsed by the UN General Assembly; calls for UN peacekeeping missions to be reinforced with cyber defence capacities in line with the effective implementation of their mandates;

UN, ***including through the proposition of a Programme of Action***, to help truly promote responsible state behaviour in cyber space, building on the consensus reports of the UN GGE endorsed by the UN General Assembly; ***welcomes the recommendations of the OEWG final report, notably on the establishment of a Programme of Action***; calls for UN peacekeeping missions to be reinforced with cyber defence capacities in line with the effective implementation of their mandates;

Or. en

Amendment 250
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 26

Motion for a resolution

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

Amendment

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

Or. en

Amendment 251
Urmas Paet, Christophe Grudler, Michal Šimečka, Nicolae Ștefănuță, Klemen Grošelj

Motion for a resolution
Paragraph 26

Motion for a resolution

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

Amendment

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

Or. en

Amendment 252

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 26 a (new)

Motion for a resolution

Amendment

26 a. Underlines the important role of cyber diplomacy in the EU toolbox; considers that striving to secure multilateral agreements on cyber norms, responsible state and non-state behaviour in cyberspace and effective global digital governance as well as creating an open, free, stable and secure cyberspace anchored in international law through alliances between like-minded countries, organisations, the private sector, civil society and experts, it's an integral part of a more comprehensive cyber-defence strategy;

Or. en

Amendment 253

Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 26 a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 254
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 26 a (new)

Motion for a resolution

Amendment

26 a. Welcomes the importance attributed to a global, open, free, stable and secure cyber space underlined by the 19 April 2021 EU Strategy for cooperation in the Indo-Pacific; calls for actively developing closer ties with likeminded democracies in the Indo-Pacific region, such as the United States, South Korea, Japan, India, Australia and Taiwan in order to share knowledge and experience as well as exchange information on countering cyber threat;

Or. en

Amendment 255
Lukas Mandl, Henna Virkkunen
on behalf of the PPE Group
Rasa Juknevičienė

Motion for a resolution
Paragraph 26 b (new)

Motion for a resolution

Amendment

26 b. Underlines the importance of cooperation with other countries, particularly in the EU's immediate neighbourhood, to help build up their capacity to defend against cybersecurity threats; commends the Commission's support for cybersecurity programmes in the Western Balkans and the Eastern Partnership countries;

Or. en

Amendment 256
Juozas Olekas, Attila Ara-Kovács

Motion for a resolution
Paragraph 26 b (new)

Motion for a resolution

Amendment

26 b. Underlines the importance of cooperation with National Parliaments in order to exchange best practices of the area of cyber defence;

Or. en

Amendment 257
Emmanuel Maurel

Motion for a resolution
Paragraph 27

Motion for a resolution

Amendment

27. Instructs its President to forward

27. Instructs its President to forward

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

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 and the national parliaments of the Member States.

Or. fr