



2018/2004(INI)

11.4.2018

AMENDMENTS

1 - 338

Draft report
Urmas Paet
(PE618.310v01-00)

on Cyber defence
(2018/2004(INI))

Amendment 1

Marietje Schaake, Urmas Paet, Javier Nart, Patricia Lalonde, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Citation 13 a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 2

Marietje Schaake, Urmas Paet, Javier Nart, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Citation 13 b (new)

Motion for a resolution

Amendment

- *having regard to the work of the Global Commission on the Stability of Cyberspace,*

Or. en

Amendment 3

María Teresa Giménez Barbat

Motion for a resolution

Citation 15 a (new)

Motion for a resolution

Amendment

- *having regard to its resolution of 3 October 2017 on the fight against Cybercrime,*

Amendment 4
Andrea Bocskor

Motion for a resolution
Citation 16

Motion for a resolution

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

Amendment

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

Or. en

Amendment 5
Tunne Kelam

Motion for a resolution
Citation 16 a (new)

Motion for a resolution

Amendment

- *having regard to its resolution of 22 November 2012 on Cyber Security and Defence (2012/2096(INI)),*

Or. en

Amendment 6
Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Patricia Lalonde, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution
Citation 17 a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 7
Tunne Kelam

Motion for a resolution
Recital -A (new)

Motion for a resolution

Amendment

-A. *whereas cyber and hybrid challenges, threats and attacks constitute a major threat to the security, defence, stability and competitiveness of the EU, its Member States and its citizens; whereas cyber defence clearly incorporates both military and civilian dimensions;*

Or. en

Amendment 8
Tunne Kelam

Motion for a resolution
Recital -A a (new)

Motion for a resolution

Amendment

-Aa. *whereas the EU and the Member States face an unprecedented threat in the*

form of politically motivated state-sponsored cyber-attacks as well as cyber-crime and terrorism;

Or. en

Amendment 9
Tunne Kelam

Motion for a resolution
Recital -A b (new)

Motion for a resolution

Amendment

-Ab. whereas cyber space is widely recognized as the 5th operational domain by the military enabling the development of cyber defence capabilities; whereas debates are held whether to recognize cyber space as the 5th domain of warfare;

Or. en

Amendment 10
Tunne Kelam

Motion for a resolution
Recital -A c (new)

Motion for a resolution

Amendment

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

whereas the solidarity clause implies the use of both civilian and military structures;

Or. en

Amendment 11

Tunne Kelam

Motion for a resolution

Recital -A d (new)

Motion for a resolution

Amendment

-Ad. whereas while cyber defence remains a core competence of the Member States, the EU has a crucial role to play in providing a platform for European cooperation and in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts;

Or. en

Amendment 12

Ana Gomes

Motion for a resolution

Recital A

Motion for a resolution

Amendment

A. whereas the cyber defence of Europe's armed forces *has* become *one of the* critical *issues* in debates about defence modernisation and Europe's common defence efforts;

A. whereas the cyber defence of Europe's armed forces *and critical infrastructures have* become *a* critical *issue* in debates about defence modernisation and Europe's common defence efforts *and enhancing the strategic autonomy of the European Union;*

Or. en

Amendment 13
Anna Elżbieta Fotyga

Motion for a resolution
Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the **critical** issues in debates about defence **modernisation and Europe's common defence efforts**;

Amendment

A. whereas the cyber defence of Europe's armed forces **and critical infrastructure** has become one of the **crucial** issues in debates about defence **modernization**;

Or. en

Amendment 14
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Amendment

A. whereas the **term** cyber defence **has not yet been defined at EU level and its implications in terms of policies, its offensive, or defensive nature, its budgets, institutions and personnel remain unclear**; whereas **resilience against cyber attacks** of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Or. en

Amendment 15
Fabio Massimo Castaldo

Motion for a resolution
Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Amendment

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts *as well as a key element for future developments of the armed forces and their operations*;

Or. en

Amendment 16

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Amendment

A. whereas the cyber defence *and deterrence* of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Or. en

Amendment 17

Jean-Luc Schaffhauser

Motion for a resolution

Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and *Europe's* common defence efforts;

Amendment

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and *Member States'* common defence efforts;

Or. fr

Amendment 18
Victor Boştinaru

Motion for a resolution
Recital A

Motion for a resolution

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts;

Amendment

A. whereas the cyber defence of Europe's armed forces has become one of the critical issues in debates about defence modernisation and Europe's common defence efforts; ***whereas the current vulnerability is mostly due to the fragmentation of our European defence strategies and capabilities;***

Or. en

Amendment 19
Victor Boştinaru

Motion for a resolution
Recital A a (new)

Motion for a resolution

Aa. whereas EU Member States are often subject to cyber attacks conducted by state and non-state actors that represent a threat to their political, civil, economic and military security, and that are in some cases part of a hybrid warfare; whereas such attacks, no matter if they have military or civilian targets, are equally dangerous and consequently need a coordinated response at civil and military level; whereas it is essential to protect critical civilian and military infrastructure, and key institutions and entities;

Or. en

Amendment 20
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Recital A a (new)

Motion for a resolution

Amendment

Aa. whereas intelligence agencies have repeatedly exploited security vulnerabilities of IT systems in order to gather intelligence; whereas governments and their agencies have failed to inform citizens, manufacturers and other stakeholders in due time in order to allow them to address the vulnerabilities in their corresponding products and services; whereas this modus operandi relies on the risky assumption that no hostile actor discovers these vulnerabilities in parallel;

Or. en

Amendment 21
Arnaud Danjean

Motion for a resolution
Recital A a (new)

Motion for a resolution

Amendment

Aa. whereas repeated cyber-attacks have revealed vulnerabilities in networks that are essential to EU security; whereas these attacks make stepping up the defence and development of EU offensive and defensive capabilities a matter of priority;

Or. fr

Amendment 22
Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution
Recital A a (new)

Motion for a resolution

Amendment

Aa. whereas cyber defence is of importance for the military, but more generally it is important for governments, industries, consumers and citizens as cyber incidents have a strong economic and societal impact;

Or. en

Amendment 23
Eva Kaili, Nikos Androulakis

Motion for a resolution
Recital A a (new)

Motion for a resolution

Amendment

Aa. whereas the lines between civil and military interference become blurry in the cyberspace;

Or. en

Amendment 24
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Recital A b (new)

Motion for a resolution

Amendment

Ab. whereas there is neither a fully-fledged defensive nor an offensive cyber defence policy which is currently operational at the EU level; whereas an offensive cyber defence policy can include elements, approaches and instruments whose use can amount to being

*considered a breach of international law;
whereas the EU is best placed to develop a
defensive cyber defence which primarily
relies on highly resilient systems and
strong restrictive economic counter
measures such as sanctions against
persons or states;*

Or. en

Amendment 25

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital A c (new)

Motion for a resolution

Amendment

Ac. whereas a large number of cyber incidents occur due to lack of resilience and robustness of private and public network infrastructure, poorly protected or secured databases and other flaws in the critical information infrastructure; whereas only few Member States consider the protection of their network and information systems and associated data as part of their respective duty of care which explains the lack of investment in state-of-the art security technology, training and the development of appropriate guidelines;

Or. en

Amendment 26

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital A d (new)

Motion for a resolution

Amendment

Ad. *whereas the rights to privacy and data protection are laid down in the EU Charter and Article 16 TFEU and are regulated by the EU's General Data Protection Regulation whose entry into application will be May 2018;*

Or. en

Amendment 27

Fabio Massimo Castaldo

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up **well-staffed** cyber commands to meet these new challenges; whereas cyber defence is an activity that **can best** be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. whereas several Member States have invested substantially in setting up cyber commands to meet these new challenges; whereas cyber defence is an activity that **could** be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries; **whereas there is still a lack of clear and common vocabulary related to cyberspace;**

Or. en

Amendment 28

Geoffrey Van Orden

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is

an activity that can best be tackled cooperatively *as its operational domain recognises neither national nor organisational boundaries*;

an activity that can best be tackled cooperatively;

Or. en

Amendment 29

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet *these* new challenges; whereas cyber *defence* is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet new challenges; whereas cyber *commands of Member States vary as regards their offensive or defensive mandate; whereas in particular strengthening resilience against cyber attacks* is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Or. en

Amendment 30

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence *is* an activity that can best be tackled cooperatively as its operational domain recognises neither national nor

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence *and deterrence are* an activity that can best be tackled cooperatively as its operational domain recognises neither national nor

organisational boundaries;

organisational boundaries;

Or. en

Amendment 31
Victor Boştinaru

Motion for a resolution
Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. *whereas we have a largely unregulated and unregulated cyberspace and cyber attacks are targeting several countries and have a cross border impact,* whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges *but a lot remains to be done as it is more and more difficult to counter cyber attacks at the Member State level;* whereas cyber defence is an activity that can best be tackled cooperatively *at an European level and in coordination with our partners and allies* as its operational domain recognises neither national nor organisational boundaries;

Or. en

Amendment 32
Jean-Luc Schaffhauser

Motion for a resolution
Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain

recognises neither national nor organisational boundaries;

recognises neither national nor organisational boundaries; *whereas cyber defence is nonetheless an area in which Member States have sovereignty and being dependent technologically in this field on another Member State entails a loss of sovereignty;*

Or. fr

Amendment 33

Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges *and improve cyber resilience*; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Or. en

Amendment 34

Marietje Schaake, Urmas Paet, Javier Nart, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain

recognises neither national nor organisational boundaries;

recognises neither national nor organisational boundaries; *whereas the majority of knowledge about operating and securing data systems, software and networks is overwhelmingly in the hands of private companies, which creates fundamental governance and security questions about the ability of states to defend their citizens;*

Or. en

Amendment 35
Bogdan Andrzej Zdrojewski

Motion for a resolution
Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries; *whereas cyber defence does not distinguish between military and civilian tasks, and therefore requires synergies between civil and military specialists in order to undertake it;*

Or. pl

Amendment 36
Arne Lietz, Eugen Freund

Motion for a resolution
Recital B

Motion for a resolution

B. whereas several Member States

Amendment

B. whereas several Member States

have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

have invested substantially in setting up well-staffed cyber commands to meet these new challenges; ***whereas at the same time, cyber defence structures remain fragmented and vary broadly amongst Member States***; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Or. en

Amendment 37
Urmas Paet

Motion for a resolution
Recital B

Motion for a resolution

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Amendment

B. whereas several Member States have invested substantially in setting up well-staffed cyber commands to meet these new challenges; ***however much more needs to be done***; whereas cyber defence is an activity that can best be tackled cooperatively as its operational domain recognises neither national nor organisational boundaries;

Or. en

Amendment 38
Bogdan Andrzej Zdrojewski

Motion for a resolution
Recital B a (new)

Motion for a resolution

Ba. whereas there is an urgent need to strengthen capabilities in the field of cyber defence due to the lack of a timely response to the changing cyber security

Amendment

landscape; whereas rapid response and adequate preparedness are key elements in ensuring security in this area;

Or. pl

Amendment 39
Tunne Kelam

Motion for a resolution
Recital C

Motion for a resolution

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;

deleted

Or. en

Amendment 40
Jean-Luc Schaffhauser

Motion for a resolution
Recital C

Motion for a resolution

Amendment

*C. whereas while cyber defence remains a core competence of the Member States, the EU has a **vital** role to play in ensuring that **these new** endeavours are **closely** coordinated **from the start** to avoid the inefficiencies that mark many **traditional** defence efforts; **whereas a substantial cyber defence capability is a necessary part of the development of the***

*C. whereas while cyber defence remains a core competence of the Member States, the EU has a role to play in ensuring that **Member State** endeavours are coordinated to avoid the inefficiencies that mark many defence **coordination** efforts;*

Amendment 41
Geoffrey Van Orden

Motion for a resolution
Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a **vital** role to play in ensuring that these new endeavours are closely coordinated **from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;**

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a role to play in ensuring that these new endeavours are closely coordinated **and that its efforts complement and do not duplicate those of NATO;**

Amendment 42
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Recital C

Motion for a resolution

C. whereas **while** cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that **these new endeavours** are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas **a substantial cyber defence capability** is a necessary part of the development of **the European Defence Union;**

Amendment

C. whereas cyber defence remains a core competence of the Member States **as all military activities according to the Treaty**, the EU has a vital role to play in ensuring that **in particular defence against cyber attacks on armed forces** are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas **close coordination on protecting armed forces against cyber attacks** is a necessary part of

the development of *an effective CSDP*;

Or. en

Amendment 43
Victor Boştinaru

Motion for a resolution
Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas *a* substantial cyber defence capability *is* a necessary part of the development of the European Defence Union;

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas *we need to do more than enhancing our cooperation and coordination; whereas we have to ensure effective prevention through steeping up the ability of the EU to detect, defend and deter in order to avoid that some states least prepared become an easy target of cyber attacks, whereas* substantial cyber defence capability *should be* a necessary part of *the Common Defence and Security Policy and* the development of the European Defence Union;

Or. en

Amendment 44
Anna Elżbieta Fotyga

Motion for a resolution
Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU *has a vital role to play in*

Amendment

C. whereas while cyber defence remains a core competence of the Member States, *coordination at an international*

ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of *the European Defence Union*;

level, namely via NATO and with close cooperation with the EU, *is vital in order* to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of *armed forces in Europe*;

Or. en

Amendment 45
Arne Lietz, Eugen Freund

Motion for a resolution
Recital C

Motion for a resolution

C. whereas *while cyber defence remains a core competence of the Member States*, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;

Amendment

C. whereas the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;

Or. en

Amendment 46
Fabio Massimo Castaldo

Motion for a resolution
Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid *the* inefficiencies that mark many

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid *gaps and* inefficiencies that mark many

traditional defence efforts; whereas a substantial cyber defence capability *is* a necessary part of the development of the European Defence Union;

traditional defence efforts; whereas a substantial cyber defence capability *should be* a necessary part of the development of the European Defence Union;

Or. en

Amendment 47

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence *capability* is a necessary part of the development of the European Defence Union;

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a *credible cyber defence and deterrence is needed for achieving effective cybersecurity for the EU and a* substantial cyber defence *capacity* is a necessary part of the development of the European Defence Union;

Or. en

Amendment 48

Bogdan Andrzej Zdrojewski

Motion for a resolution

Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many

traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;

traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union; ***whereas we are facing a permanent shortage of highly qualified cyber defence specialists;***

Or. pl

Amendment 49

Marietje Schaake, Javier Nart, Urmas Paet, Patricia Lalonde, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Recital C

Motion for a resolution

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union;

Amendment

C. whereas while cyber defence remains a core competence of the Member States, the EU has a vital role to play in ensuring that these new endeavours are closely coordinated from the start to avoid the inefficiencies that mark many traditional defence efforts; whereas a substantial cyber defence capability is a necessary part of the development of the European Defence Union; ***whereas the protection of our network and information security is a core competence of the European Union and should be an essential part of the European Digital Single Market;***

Or. en

Amendment 50

Anna Elżbieta Fotyga

Motion for a resolution

Recital C a (new)

Motion for a resolution

Amendment

Ca. whereas the 2016 NATO Summit

Declaration of Warsaw recognised cyberspace as a domain of operations in which NATO must defend itself as effectively as it does in the air, on land and at sea;

Or. en

Amendment 51
Victor Boştinaru

Motion for a resolution
Recital C a (new)

Motion for a resolution

Amendment

Ca. whereas an active and efficient cyberpolicy is one that allows deterring enemies as well as disrupting capabilities, pre-empting and degrading the ability to attack;

Or. en

Amendment 52
Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Patricia Lalonde, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš, Nadja Hirsch

Motion for a resolution
Recital D

Motion for a resolution

Amendment

D. whereas the EU has contributed in improving Member States cyber defence capabilities, **both** through dual-use research **and** projects coordinated by the European Defence Agency (EDA);

D. whereas the EU has contributed in improving Member States cyber defence capabilities, through dual-use research, projects coordinated by the European Defence Agency (EDA) **and in improving Member States cyber resilience, through support provided by the EU Cyber Security Agency (ENISA);**

Or. en

Amendment 53
Geoffrey Van Orden

Motion for a resolution
Recital D

Motion for a resolution

D. whereas the EU *has* contributed in improving Member States cyber defence capabilities, both through dual-use research and projects coordinated by the European Defence Agency (EDA);

Amendment

D. whereas the EU *and NATO have* contributed in improving *their* Member States' cyber defence capabilities, both through dual-use research and projects coordinated by the European Defence Agency (EDA) *and NATO*;

Or. en

Amendment 54
Jean-Luc Schaffhauser

Motion for a resolution
Recital E

Motion for a resolution

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to facilitate cooperative projects in the cyber defence *domain*;

Amendment

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to facilitate cooperative projects in the *field of* cyber defence, *for which, however, the legitimate authorities of each Member State concerned retain sole competence, and whereas in this field the European Union should simply record Member State coordination or if necessary encourage its establishment but its role should not extend beyond this*;

Or. fr

Amendment 55
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Recital E

Motion for a resolution

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to facilitate cooperative projects in the cyber defence domain;

Amendment

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope ***to foster an ecosystem that can provide opportunities for SMEs and startup companies, and*** to facilitate cooperative projects in the cyber defence domain;

Or. en

Amendment 56

Victor Boştinaru

Motion for a resolution

Recital E

Motion for a resolution

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to facilitate cooperative projects in the cyber defence domain;

Amendment

E. whereas both Permanent Structured Cooperation (PESCO) and the European Defence Fund (EDF) are new initiatives with the necessary scope to facilitate cooperative projects in the cyber defence domain ***and will contribute to shape the regulatory and institutional framework;***

Or. en

Amendment 57

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital F

Motion for a resolution

F. whereas Member States participating in PESCO have committed

Amendment

F. whereas Member States participating in PESCO have committed

themselves to ensuring that cooperation efforts on cyber defence – *such as information sharing, training and operational support* – will continue to grow;

themselves to ensuring that cooperation efforts on cyber defence will continue to grow; *whereas 2 of the 17 PESCO projects are on cyber defence with a Cyber Threats and Incident Response Information Sharing Platform and a Cyber Rapid Response Teams and Mutual Assistance in Cyber Security project, which both focus on information sharing, risk mitigation, higher levels of cyber resilience and collective response to incidents;*

Or. en

Amendment 58
Jean-Luc Schaffhauser

Motion for a resolution
Recital F

Motion for a resolution

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

Amendment

F. whereas Member States participating in PESCO have committed themselves to ensuring that cooperation efforts on cyber defence – such as information sharing, training and operational support – will continue to grow; *whereas each Member State has full sovereignty over information classified as ‘confidential defence’ or ‘secret defence’ and whereas said information should not be shared with private companies or companies linked to mercenary practices;*

Or. fr

Amendment 59
Urmas Paet

Motion for a resolution
Recital F a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 60
Fabio Massimo Castaldo

Motion for a resolution
Recital G

Motion for a resolution

Amendment

G. whereas training needs in the area of cyber defence are substantial and increasing, and ***are most efficiently met cooperatively*** at the European level;

G. whereas training needs in the area of cyber defence are substantial and increasing, and ***require more joint efforts*** at the European level;

Or. en

Amendment 61
Anna Elżbieta Fotyga

Motion for a resolution
Recital G

Motion for a resolution

Amendment

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the ***European*** level;

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the ***EU and NATO*** level;

Or. en

Amendment 62
Geoffrey Van Orden

Motion for a resolution

Recital G

Motion for a resolution

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively **at the European level**;

Amendment

G. whereas training needs in the area of cyber defence are substantial and increasing, and are **often** most efficiently met cooperatively;

Or. en

Amendment 63

Ana Gomes

Motion for a resolution

Recital G

Motion for a resolution

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the European level;

Amendment

G. whereas **capacity building and** training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the European level;

Or. en

Amendment 64

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital G

Motion for a resolution

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the European level;

Amendment

G. whereas training needs in the area of cyber defence are substantial and increasing, and are most efficiently met cooperatively at the European **or Transatlantic** level;

Or. en

Amendment 65
Urmas Paet

Motion for a resolution
Recital G a (new)

Motion for a resolution

Amendment

Ga. whereas the European Defence Fund (EDF) needs to support the global competitiveness and innovativeness of the European defence industry by investing in digital and cyber technologies as well as provide opportunities for SMEs and start-up companies to participate in order to facilitate development of smart solutions;

Or. en

Amendment 66
Urmas Paet

Motion for a resolution
Recital H

Motion for a resolution

Amendment

H. whereas the EDA has launched a number of projects to meet Member States' need for cyber defence capability development, including on education and training;

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

Or. en

Amendment 67
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Recital H

Motion for a resolution

H. whereas the EDA has launched a number of projects to meet Member States' need for cyber defence capability development, including on education **and** training;

Amendment

H. whereas the EDA has launched a number of projects to meet Member States' need for cyber defence capability development, including on education, training **and doctrine-support**;

Or. en

Amendment 68

Urmas Paet

Motion for a resolution

Recital H a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 69

Jean-Luc Schaffhauser

Motion for a resolution

Recital I

Motion for a resolution

Amendment

I. whereas the European Security and Defence College (ESDC) network is the **only European** training provider for **the CSDP structures, missions and operations**; whereas its role in pooling European training capacities **is planned to**

I. whereas the European Security and Defence College (ESDC) network is **one of** the training **providers, alongside other national facilities**, for **Member State military academies**; whereas its role in pooling European training capacities **could**

be substantially increased in the *cyber* domain;

be substantially increased in the *cyber-defence threats and tools* domain;

Or. fr

Amendment 70
Geoffrey Van Orden

Motion for a resolution
Recital I

Motion for a resolution

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

Amendment

I. whereas the European Security and Defence College (ESDC) network is *a* European training provider for the CSDP structures, missions and operations; whereas its role in pooling European training capacities is planned to be substantially increased in the cyber domain;

Or. en

Amendment 71
Jean-Luc Schaffhauser

Motion for a resolution
Recital J

Motion for a resolution

J. whereas the EU and NATO *have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016;*

Amendment

J. whereas the EU and NATO *are not subject to the same threats – some members of NATO even go so far as to spy electronically on other EU Member States – and therefore NATO does not constitute a partner but a threat, for which reason for a common cybersecurity policy to be effective, it is absolutely essential that it be implemented outside NATO;*

Or. fr

Amendment 72
Victor Boştinaru

Motion for a resolution
Recital J

Motion for a resolution

J. whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016;

Amendment

J. ***whereas the EU and NATO are complementary partners in building their cyber resilience; whereas cyber security and defence is already one of the strongest pillars of cooperation between the two and a critical field where both have unique capacities and they should therefore step up cooperation, including through joint exercises; whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016;***

Or. en

Amendment 73
Urmas Paet

Motion for a resolution
Recital J

Motion for a resolution

J. whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016;

Amendment

J. whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016; ***whereas four out of forty two proposals for closer cooperation concern cyber security and defence, with further proposals aiming at hybrid threats more broadly; whereas this has been complemented by a further proposal regarding cyber security and defence on 5 December 2017;***

Or. en

Amendment 74
Bogdan Andrzej Zdrojewski

Motion for a resolution
Recital J

Motion for a resolution

J. whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016;

Amendment

J. whereas the EU and NATO have agreed to a broad agenda of cooperation in the EU-NATO Joint Declaration of 8 July 2016; ***whereas in 2014, NATO established cyber security as part of the Alliance's core collective defence activities, and in 2016 it identified cyberspace as an operational domain alongside land, air and sea;***

Or. pl

Amendment 75
Urmas Paet

Motion for a resolution
Recital J a (new)

Motion for a resolution

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

Or. en

Amendment 76
Ana Gomes

Motion for a resolution

Recital K

Motion for a resolution

K. whereas command and control systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors seeking to attack missions;

Amendment

K. whereas command and control systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors seeking to attack missions ***and critical infrastructures of Member States and the Union;***

Or. en

Amendment 77

Geoffrey Van Orden

Motion for a resolution

Recital K

Motion for a resolution

K. whereas command and control systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors ***seeking to attack missions;***

Amendment

K. whereas command and control systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors ***and therefore need to be adequately protected;***

Or. en

Amendment 78

Eugen Freund

Motion for a resolution

Recital K

Motion for a resolution

K. whereas command and control

Amendment

K. whereas command and control

systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors seeking to attack missions;

systems, information exchange and logistics rely on classified and unclassified IT infrastructure, especially at the tactical and operational level; whereas these systems are attractive targets for malicious actors seeking to attack missions; ***whereas cyber-attacks may have serious repercussions for infrastructure in the European Union; whereas, in particular, the European Union's energy infrastructure may be a target for cyber-attacks with serious repercussions and must therefore be particularly protected against such attacks;***

Or. de

Amendment 79
Fabio Massimo Castaldo

Motion for a resolution
Recital K a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 80
Geoffrey Van Orden

Motion for a resolution

Recital L

Motion for a resolution

L. whereas cyber defence is an important consideration at all stages of the planning process, and *whereas* adequate capabilities need to be available to ***mainstream it fully into mission planning and*** provide critical support;

Amendment

L. whereas ***it is well understood that*** cyber defence is an important consideration at all stages of the planning process, and ***that*** adequate capabilities need to be available to provide ***the necessary*** critical support;

Or. en

Amendment 81

Fabio Massimo Castaldo

Motion for a resolution

Recital L

Motion for a resolution

L. whereas cyber defence ***is an important consideration*** at all stages of the planning process, and whereas adequate capabilities need to be available ***to mainstream it fully*** into mission planning and provide critical support;

Amendment

L. whereas cyber defence ***should be duly considered*** at all stages of the planning process, and whereas adequate capabilities need to be available into mission planning and provide critical support;

Or. en

Amendment 82

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Recital L

Motion for a resolution

L. whereas cyber defence is an important consideration at all stages of the planning process, and whereas adequate ***capabilities need*** to be available to mainstream it fully into mission planning

Amendment

L. whereas cyber defence is an important consideration at all stages of the planning process, and whereas ***an adequate level of resilience needs*** to be available to mainstream it fully into ***CSDP*** mission ***and***

and provide critical support;

operations planning and provide critical support;

Or. en

Amendment 83

Clare Moody, Wajid Khan

Motion for a resolution

Recital L

Motion for a resolution

L. whereas cyber defence is an important consideration at all stages of the planning process, and whereas adequate capabilities need to be available to mainstream it fully into mission planning and provide critical support;

Amendment

L. whereas cyber defence is an important consideration at all stages of the planning process *as well as requiring constant monitoring*, and whereas adequate capabilities need to be available to mainstream it fully into mission planning and provide *continuous* critical support;

Or. en

Amendment 84

Marietje Schaake, Javier Nart, Urmas Paet, Patricia Lalonde, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Recital M

Motion for a resolution

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it failed to arrive at a consensus report *this time*, the 2015 and 2013 agreements still apply, in that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and to promoting an open, secure, peaceful and accessible cyberspace;

Amendment

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it failed to arrive at a consensus report *in 2017*, the 2015 and 2013 agreements still apply, in that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and to promoting an open, secure, peaceful and accessible cyberspace; *whereas the*

European Union should actively engage in norm-setting initiatives that promote responsible state behaviour in cyberspace outside the UN when the UN GGE process is dormant;

Or. en

Amendment 85
Urmas Paet

Motion for a resolution
Recital M

Motion for a resolution

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it **failed to arrive at** a consensus report this time, the 2015 and 2013 agreements **still** apply, **in** that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, **and to** promoting an open, secure, peaceful and accessible **cyberspace**;

Amendment

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it **was not able to produce** a consensus report this time, the 2015 and 2013 agreements apply, **including** that international law, **and** in particular the Charter of the United Nations, is applicable and **is** essential to maintaining peace and stability **and** promoting an open, secure, peaceful and accessible **ICT environment**;

Or. en

Amendment 86
Andrea Bocskor

Motion for a resolution
Recital M

Motion for a resolution

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it failed to arrive at a consensus report this time, the 2015 and 2013 **agreements** still

Amendment

M. whereas the UN Group of Governmental Experts on Information Security (UNGGE) has concluded its last round of deliberation; whereas even though it failed to arrive at a consensus report this time, the 2015 and 2013 **reports** still apply,

apply, in that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and to promoting an open, secure, peaceful and accessible *cyberspace*;

in that *existing* international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability, and to promoting an open, secure, peaceful and accessible *ICT environment*;

Or. en

Amendment 87
Andrea Bocskor

Motion for a resolution
Recital N

Motion for a resolution

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

Amendment

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

Or. en

Amendment 88
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, *among others* – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure,

Amendment

O. whereas different state actors – Russia, China and North Korea, *but also security agencies, and private companies some of which are based on the territory of allies* – have been involved in malicious cyber activities in pursuit of political, *mass*

cyber-espionage, disinformation campaigns and limiting access to the internet (*such as Wannacry, NonPetya*); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

surveillance of EU citizens, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet *and the functioning of IT systems*; whereas such activities could constitute wrongful acts under international law, *violations of international human rights law, EU fundamental rights* and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox *or in case of private companies restricted access to the internal market including fines*;

Or. en

Amendment 89 Ana Gomes

Motion for a resolution Recital O

Motion for a resolution

O. whereas different state actors – Russia, China *and* North Korea, among others – have been involved in *malicious* cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities *could constitute wrongful acts under* international law and *could lead to* a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, China, North Korea, *Israel, the United States*, among others – have been involved in cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya, *Stuxnet*); whereas such activities *disregard and violate* international law and *can jeopardise democracy, security, public order and the strategic autonomy of the European Union, therefore calling for* a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 90
Anna Elżbieta Fotyga

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, *such as using the EU cyber diplomacy toolbox*;

Amendment

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas *these attacks are also often conducted by the non-state actors (such as criminal groups), inspired or hired by such states; whereas also terrorist organisations have gained capabilities of performing such attacks; whereas* such activities could constitute wrongful acts under international law and could lead to a joint EU *and NATO* response;

Or. en

Amendment 91
Andrea Bocskor

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – *Russia, China and North Korea, among others* – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, *NonPetya*); *whereas such activities could constitute wrongful acts*

Amendment

O. whereas different state actors, *non state actors and state-sponsored actors* have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, *NotPetya*);

under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 92
Clare Moody, Wajid Khan

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, *NonPetya*); whereas such activities *could* constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, *aiding* disinformation campaigns and limiting access to the internet (such as Wannacry, *for which North Korea is culpable and NotPetya, for which Russia is culpable*); whereas such activities constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 93
Urmas Paet

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that

Amendment

O. whereas different *non-state and* state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives

include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the *EU* cyber *diplomacy toolbox*;

that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the *framework for a joint EU diplomatic response to malicious cyber activities*;

Or. en

Amendment 94

Marietje Schaake, Urmas Paet, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (*such as Wannacry, NonPetya*); whereas such activities *could* constitute wrongful acts under international law and *could* lead to a joint EU response, *such as using* the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, China, *Iran* and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure (*such as Wannacry, NonPetya*), cyber-espionage, disinformation campaigns and limiting access to the internet ; whereas such activities constitute wrongful acts under international law and *should* lead to a joint EU response, *including the use of restrictive measures as envisaged by* the EU cyber diplomacy toolbox;

Or. en

Amendment 95

Fabio Massimo Castaldo

Motion for a resolution

Recital O

Motion for a resolution

O. whereas different state actors – ***Russia, China and North Korea, among others*** – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (***such as Wannacry, NonPetya***); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet; whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 96
Arnaud Danjean

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – ***Russia, China and North Korea, among others*** – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. fr

Amendment 97
Georgios Epitideios

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – ***Russia, China and North Korea, among others*** – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. el

Amendment 98
Arne Lietz, Eugen Freund

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – ***Russia, China and North Korea, among others*** – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 99
Eva Kaili, Nikos Androulakis

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, **Turkey**, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 100
Tunne Kelam

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, China, **Iran** and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment 101
Geoffrey Van Orden

Motion for a resolution
Recital O

Motion for a resolution

O. whereas different state actors – Russia, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Amendment

O. whereas different state actors – Russia, **Iran**, China and North Korea, among others – have been involved in malicious cyber activities in pursuit of political, economic or security objectives that include attacks on critical infrastructure, cyber-espionage, disinformation campaigns and limiting access to the internet (such as Wannacry, NonPetya); whereas such activities could constitute wrongful acts under international law and could lead to a joint EU response, such as using the EU cyber diplomacy toolbox;

Or. en

Amendment 102
Urmas Paet

Motion for a resolution
Recital O a (new)

Motion for a resolution

Oa. whereas cyber security technologies ("dual-use" technologies) are relevant to the military and civilian domains and offer many opportunities to develop synergies between civilian and military actors in a number of areas, such as for example encryption, security and vulnerability management tools, intrusion detection and prevention systems;

Amendment 103
Anna Elżbieta Fotyga

Motion for a resolution
Recital O a (new)

Motion for a resolution

Amendment

Oa. whereas such attacks on a large scale were performed numerous times in the past, including against Estonia in 2007, Georgia in 2008, and currently are being used almost on a daily basis against Ukraine; whereas offensive cyber capabilities are also being employed against EU and NATO Member States at an unprecedented scale;

Or. en

Amendment 104
Fabio Massimo Castaldo

Motion for a resolution
Recital O a (new)

Motion for a resolution

Amendment

Oa. whereas the development of cyber technologies during the next years will affect new fields, like artificial intelligence, the internet of things, robotics and mobile devices, and all these elements could also present several security implications for the defence domain;

Or. en

Amendment 105
Urmas Paet

Motion for a resolution
Recital O b (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 106
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Subheading 1

Motion for a resolution

Amendment

Capability development for cyber defence

Capability development for cyber defence
deterrence

Or. en

Amendment 107
Tunne Kelam

Motion for a resolution
Paragraph -1 (new)

Motion for a resolution

Amendment

-1. *Underlines that common cyber defence policy and substantial cyber defence capability should constitute one of the cores of the development of the European Defence Union;*

Or. en

Amendment 108
María Teresa Giménez Barbat

Motion for a resolution
Paragraph -1 (new)

Motion for a resolution

Amendment

-1 Welcomes the initiative of the European Commission for a cybersecurity package to foster EU cyber resilience, deterrence and defence;

Or. en

Amendment 109
Tunne Kelam

Motion for a resolution
Paragraph -1 a (new)

Motion for a resolution

Amendment

-1a. Recalls that cyber defence has both military and civilian dimensions and that this requires an integrated policy approach and close cooperation between military and civilian stakeholders;

Or. en

Amendment 110
Tunne Kelam

Motion for a resolution
Paragraph -1 b (new)

Motion for a resolution

Amendment

-1b. Strongly emphasises that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely

integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Or. en

Amendment 111
Tunne Kelam

Motion for a resolution
Paragraph -1 c (new)

Motion for a resolution

Amendment

-1c. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State and therefore efforts to pursue a common cyber defence policy should be intensified;

Or. en

Amendment 112
Tunne Kelam

Motion for a resolution
Paragraph -1 d (new)

Motion for a resolution

Amendment

-1d. Calls on working towards coherent development of cyber capacities across all EU institutions and bodies, as well as in Member States and on providing needed

political and practical solutions to overcome the remaining political, legislative and organisational obstacles for the cooperation on cyber defence; finds regular and enhanced exchange and cooperation between relevant public stakeholders on EU and national level in cyber defence crucial;

Or. en

Amendment 113
James Carver

Motion for a resolution
Paragraph 1

Motion for a resolution

Amendment

1. Commends the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

deleted

Or. en

Amendment 114
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 1

Motion for a resolution

Amendment

1. Commends the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for

1. Takes note of the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for

headquarters;

headquarters;

Or. en

Amendment 115

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 1

Motion for a resolution

1. *Commends* the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

Amendment

1. *Notes* the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

Or. en

Amendment 116

Urmaz Paet

Motion for a resolution

Paragraph 1

Motion for a resolution

1. Commends the work done by the **EDA and the Commission** in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

Amendment

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

Or. en

Amendment 117
David McAllister

Motion for a resolution
Paragraph 1

Motion for a resolution

1. Commends the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on cyber ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

Amendment

1. Commends the work done by the EDA and the Commission in the field of cyber defence; notes in particular the EDA projects on Cyber Ranges, the Cyber Defence Strategic Research Agenda and the development of deployable cyber situation awareness packages for headquarters;

Or. en

Amendment 118
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 1 a (new)

Motion for a resolution

Amendment

1a. Believes that there is an urgent need to clarify terminology with regards to cyber defence and cyber security and in particular at the EU level; underlines the need for a common terminology standard also on what a cyber attacks should legitimately be considered to be, before developing further cyber security and cyber defence policies at EU level;

Or. en

Amendment 119
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 1 b (new)

Motion for a resolution

Amendment

1b. Calls on the Member States and the Commission to address the issue of intentionally delayed disclosures of security vulnerabilities in a systematic and stricter manner; recalls that the nature of digital technology leaves little room for compromises and that that either all users are well-protected or they are all vulnerable; believes that the highest priority for Member States should be the duty to care about the best possible protection of their citizens, infrastructure and economic operators also in the digital age and that they are obliged to invest in highly resilient digital infrastructure and related systems;

Or. en

Amendment 120

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 1 c (new)

Motion for a resolution

Amendment

1c. Calls on the Member States and the Commission to focus on a defensive aspect of cyber defence at EU level also in order to strengthen the international rule of law and the protection of data of citizens, infrastructure and economic operators alike; underlines that the EU's cyber defence policy must rely on the one hand on preventive elements such as investments in resilience; believes on the other hand that citizens, governments, infrastructure, and economic operators are best protected in the EU in case a comprehensive toolbox is available for

responding to cyber-attacks by hostile states and criminals; stresses that it is of crucial importance to communicate clearly and publicly about all the instruments in the EU's toolbox ranging from far reaching economic sanctions to law enforcement measures;

Or. en

Amendment 121
James Carver

Motion for a resolution
Paragraph 2

Motion for a resolution

Amendment

2. Welcomes the cyber projects to be launched in the framework of PESCO, namely an information-sharing platform for cyber incidents and a rapid response team for cyber incidents;

deleted

Or. en

Amendment 122
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 2

Motion for a resolution

Amendment

2. Welcomes the cyber projects to be launched in the framework of PESCO, namely an information-sharing platform for cyber incidents and a rapid response team for cyber incidents;

2. Welcomes the *two* cyber projects to be launched in the framework of PESCO, namely an information-sharing platform for cyber incidents and a rapid response team for cyber incidents; ***underlines that these two projects focus on a defensive cyber policy which aims at sharing of cyber threat intelligence through a networked Member State platform and Cyber Rapid Response Teams (CRRTs)***

which will allow Member States to help each other to ensure higher level of cyber resilience and to collectively detect, recognise and mitigate cyber threats;

Or. en

Amendment 123
Urmas Paet

Motion for a resolution
Paragraph 2

Motion for a resolution

2. Welcomes the cyber projects to be launched in the framework of PESCO, namely an information-sharing platform for cyber incidents and *a* rapid response *team* for cyber *incidents*;

Amendment

2. Welcomes the cyber projects to be launched in the framework of PESCO, namely an information-sharing platform for cyber incidents and *cyber* rapid response *teams in* cyber *security*;

Or. en

Amendment 124
Tunne Kelam

Motion for a resolution
Paragraph 3

Motion for a resolution

3. *Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;*

Amendment

deleted

Or. en

Amendment 125
Geoffrey Van Orden

Motion for a resolution
Paragraph 3

Motion for a resolution

3. Recognises that many **Member States consider possession of their own** cyber defence capabilities **to be** at the core of **their** national security **strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;**

Amendment

3. Recognises that many cyber defence capabilities **are** at the core of national security **strategies for many countries;**

Or. en

Amendment 126
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 3

Motion for a resolution

3. **Recognises** that **many** Member States **consider** possession of **their** own cyber defence capabilities **to be at the core of their national security** strategy **and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;**

Amendment

3. **Does not just recognise but is also of the view** that **a cybersecurity policy is only possible if each Member State pursues its own policy in coordination with the other Member States, and that possession by each Member State of its own national** cyber defence capabilities **is a necessary and vital prerequisite for a common cybersecurity** strategy;

Or. fr

Amendment 127

James Carver

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; ***stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;***

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; ***supports the continuation of this approach;***

Or. en

Amendment 128

Urmas Paet

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – ***as with other military branches, and also owing*** to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that ***due*** to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces ***ensuring the strategic autonomy of the EU in cyberspace*** is beyond the reach of any single Member State;

Or. en

Amendment 129

Raffaele Fitto

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces *is beyond the reach of any single Member State*;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces *requires a coordinated response from all Member States*;

Or. it

Amendment 130

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – *the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State*;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – *there is the need to cooperate also on the European level*;

Amendment 131
David McAllister

Motion for a resolution
Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State ***and cooperative action is required to achieve the goal of EU strategic autonomy in cyberspace;***

Or. en

Amendment 132
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is

beyond the reach of any single Member State;

beyond the reach of any single Member State *and that due to EU initiatives such as the digital single market, the EU is well placed to take a leading role in developing European cyber defence strategies;*

Or. en

Amendment 133

María Teresa Giménez Barbat

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State; *calls for the development of European legal framework to address cybercrime that is compatible with fundamental rights, data protection, cybersecurity, consumer protection and e-commerce;*

Or. en

Amendment 134

Arnaud Danjean

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member

Amendment

3. Recognises that many Member

States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State; ***reiterates that development of cyber defence at EU level has to enhance the EU's capability to protect itself and act autonomously, thereby strengthening its strategic autonomy;***

Or. fr

Amendment 135
Arne Lietz, Eugen Freund

Motion for a resolution
Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State; ***notes against this backdrop that the EU and its Member States find themselves under time pressure regarding the development of such forces and need to act immediately;***

Or. en

Amendment 136

Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Patricia Lalonde, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš, Nadja Hirsch

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State; ***welcomes in this regard the proposed permanent mandate and strengthened role for ENISA;***

Or. en

Amendment 137

Marietje Schaake, Urmas Paet, Javier Nart, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Paragraph 3

Motion for a resolution

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment

3. Recognises that many Member States consider possession of their own cyber defence capabilities to be at the core of their national security strategy and to constitute an essential part of their national sovereignty; stresses, however, that – as with other military branches, and also owing to the borderless nature of cyberspace – the scale ***and knowledge*** required for truly comprehensive and effective forces is beyond the reach of any single Member State;

Amendment 138
Arnaud Danjean

Motion for a resolution
Paragraph 3 a (new)

Motion for a resolution

Amendment

3a. Notes that the EU's capability to develop cyber defence projects depends on control of technologies, equipment, services, data and data processing, and has to rely on a trusted industry stakeholder base;

Or. fr

Amendment 139
Tunne Kelam

Motion for a resolution
Paragraph 4

Motion for a resolution

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

deleted

Or. en

Amendment 140
James Carver

Motion for a resolution
Paragraph 4

Motion for a resolution

4. ***Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;***

Amendment

4. ***Supports*** Member States ***cooperation*** in the development of their respective cyber commands ***so long as this is done on a bilateral or multilateral level that is led by the Member States themselves or through NATO;***

Or. en

Amendment 141
Geoffrey Van Orden

Motion for a resolution
Paragraph 4

Motion for a resolution

4. ***Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;***

Amendment

4. ***Recognises the ambition*** in the framework of the emerging European Defence Union ***for*** cyber defence capabilities of Member States ***to*** be closely ***aligned;***

Or. en

Amendment 142
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, ***in the framework of the emerging European Defence Union***, cyber defence capabilities of Member States should be ***closely integrated from the start*** to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that ***close cooperation between Member States on enhancing the*** cyber defence capabilities of Member States should be ***encouraged in order*** to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Or. fr

Amendment 143

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 4

Motion for a resolution

4. ***Strongly emphasises, therefore, that, in the framework of*** the emerging European Defence Union, cyber defence ***capabilities*** of Member States should be closely ***integrated*** from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of ***their respective*** cyber ***commands***;

Amendment

4. ***Notes initiatives such as*** the emerging European Defence Union ***and emphasises that more concrete work still needs to be done in order to adequately strengthen*** cyber defence of Member States ***which*** should be closely ***coordinated*** from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of cyber ***defence***;

Or. en

Amendment 144

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, ***in the framework of the emerging European Defence Union***, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands; ***recognizing also that strong attribution capabilities are an essential component of effective cyber defence and cyber deterrence***;

Or. en

Amendment 145
Arnaud Danjean

Motion for a resolution
Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be ***closely*** integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate ***closely*** in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be integrated ***as far as possible*** from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate ***where possible*** in the development of their respective cyber commands;

Or. fr

Amendment 146
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands ***and that therefore cyber defence should be at the forefront of the European Defence Union;***

Or. en

Amendment 147

Arne Lietz, Eugen Freund

Motion for a resolution

Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands, ***thereby feeding into a process coordinated by the European Commission and the EDA to better streamline cyber defence structures across Member States;***

Or. en

Amendment 148

Victor Boştinaru

Motion for a resolution

Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges therefore the Member States ***to implement the short term measures that are available under the current institutional framework to identify the capabilities that should be developed urgently; also urges*** to cooperate closely in the development of their respective cyber commands ***and set a clear roadmap;***

Or. en

Amendment 149

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands; ***calls, furthermore, on the Member States to create additional common platforms for the exchange of experience and expertise in specific cyber fields;***

Or. pl

Amendment 150
María Teresa Giménez Barbat

Motion for a resolution
Paragraph 4

Motion for a resolution

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands;

Amendment

4. Strongly emphasises, therefore, that, in the framework of the emerging European Defence Union, cyber defence capabilities of Member States should be closely integrated from the start to ensure maximum efficiency; urges, therefore, the Member States to cooperate closely in the development of their respective cyber commands ; ***underlines that such cooperation should also be implemented through the enhancement of the European Union Agency for Network and Information Security (ENISA);***

Or. en

Amendment 151
Arnaud Danjean

Motion for a resolution
Paragraph 4 a (new)

Motion for a resolution

4a. Recalls that efforts to improve the homogeneity of command systems aim to have available command assets that are interoperable with NATO countries and occasional partners, and to guarantee a smooth exchange of information so as to speed up the decision-making loop and keep control of information in a cyber-risk context;

Or. fr

Amendment 152

Ivo Belet

Motion for a resolution

Paragraph 4 a (new)

Motion for a resolution

Amendment

4a. Calls on the Commission and Member States to build on the PESCO project for national Cyber Rapid Response Teams and Mutual Assistance in Cyber Security, by establishing a European Cyber Rapid Response Team to coordinate, detect and counter collective cyber threats in support of the participating Member States' efforts;

Or. en

Amendment 153

Victor Boştinaru

Motion for a resolution

Paragraph 4 a (new)

Motion for a resolution

Amendment

4a. Strongly believes effective prevention and forecasting would require big data, expertise and artificial intelligence to study patterns; Is of the opinion that we should develop an European Secure Network for critical information and infrastructure;

Or. en

Amendment 154

James Carver

Motion for a resolution

Paragraph 5

Motion for a resolution

Amendment

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

deleted

Or. en

Amendment 155

Jean-Luc Schaffhauser

Motion for a resolution

Paragraph 5

Motion for a resolution

Amendment

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

5. Urges the Member States, in this context, to propose cooperation projects;

Or. fr

Amendment 156

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 5

Motion for a resolution

Amendment

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

5. Urges the Member States, in this context, to make the best possible use of the framework provided by PESCO and ***other common initiatives*** to propose cooperation projects;

Or. en

Amendment 157

Marietje Schaake, Urmas Paet, Javier Nart, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Paragraph 5 a (new)

Motion for a resolution

Amendment

5a. Urges the Members States to increase financial and personal resources, in particular forensic experts, in order to improve the attribution of cyber attacks;

Or. en

Amendment 158

James Carver

Motion for a resolution

Paragraph 6

Motion for a resolution

Amendment

6. Recommends finding ways to complement NATO Smart Defence projects (e.g. the Multinational Cyber Defence Capability Development);

6. Recognises the leading status of NATO on defence matters; further recognises that EU led initiatives are superfluous and potentially undermine NATO;

Or. en

Amendment 159

David McAllister

Motion for a resolution

Paragraph 6

Motion for a resolution

Amendment

6. Recommends finding ways to complement NATO Smart Defence projects (e.g. the Multinational Cyber Defence Capability Development);

6. Recommends finding ways to complement NATO Smart Defence projects (e.g. the Multinational Cyber Defence Capability Development, *the Malware Information Sharing Platform (MISP) and the Multinational Cyber*

Amendment 160
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 6 a (new)

Motion for a resolution

Amendment

6a. Recognising the emerging developments in areas such as nanotechnology, artificial intelligence, big data, e-waste and advanced robotics, urges Member States and the EU to provide special attention towards the possible exploitation of these areas by hostile state actors and organized criminal groups; calls for training and capability development to protect against the emergence of sophisticated criminal schemes such as complex identity frauds and counterfeiting of goods;

Amendment 161
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 6 a (new)

Motion for a resolution

Amendment

6a. Recognizes that due to the changing environment of cyber threats, a stronger and structured cooperation with police forces could be advisable, especially in some critical areas, such as cyber-jihad, cyber-terrorism, radicalisation on line and funding of extremist or radical organisations;

Amendment 162
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 6 b (new)

Motion for a resolution

Amendment

6b. Emphasises the need for more terminological clarity about security in cyberspace, as well as a comprehensive and integrated approach and joint efforts to counter cyber and hybrid threats, to detect and eradicate online extremist and criminal safe havens, by strengthening and increasing information sharing between the EU and EU agencies such as Europol, Eurojust, EDA and ENISA;

Or. en

Amendment 163
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 6 b (new)

Motion for a resolution

Amendment

6b. Underlines the growing role of artificial intelligence in both cyber offence and defence; urges the EU and Member States to pay special attention to this area both during research and practical development of their cyber defence capabilities;

Or. en

Amendment 164
Eva Kaili, Nikos Androulakis

Motion for a resolution
Subheading 2 a (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 165
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 7

Motion for a resolution

Amendment

7. Emphasises that cyber defence should be considered an operational task for CSDP missions and operations, and that it should be included in all CSDP planning processes;

deleted

Or. fr

Amendment 166
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 7

Motion for a resolution

Amendment

7. Emphasises that cyber defence should be considered an operational task for CSDP missions and operations, and that it should be included in all CSDP planning processes;

7. Emphasises that cyber defence should be considered an operational task for CSDP missions and operations, and that it should be included in all CSDP planning processes **ensuring cyber security is constantly considered throughout the planning process thereby reducing cyber**

vulnerability gaps;

Or. en

Amendment 167
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 8

Motion for a resolution

8. Recognises that planning a successful CSDP mission or operation ***requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;***

Amendment

8. Recognises that planning a successful ***cyber defence*** mission or operation ***is a matter for countries that have the necessary expertise and skills, in order to prevent propaganda by countries manipulated within NATO;***

Or. fr

Amendment 168
Geoffrey Van Orden

Motion for a resolution
Paragraph 8

Motion for a resolution

8. Recognises that planning a successful CSDP mission or operation ***requires substantial*** cyber defence expertise, both at operational headquarters and within the mission itself, ***to conduct a thorough threat assessment and provide adequate protection in the field;*** calls ***on the EEAS, and*** on the Member States providing headquarters for CSDP operations, to strengthen their cyber

Amendment

8. Recognises that planning a successful CSDP mission or operation ***may need to include*** cyber defence expertise, both at operational headquarters and within the mission itself; calls on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

defence expertise to ensure the safety of the EU's missions;

Or. en

Amendment 169

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 8

Motion for a resolution

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and *on* the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

Amendment

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS and the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

Or. pl

Amendment 170

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 8

Motion for a resolution

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP

Amendment

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP

operations, to strengthen their cyber defence expertise to *ensure the safety of the* EU's missions;

operations, to strengthen their cyber defence expertise to EU's missions;

Or. en

Amendment 171

Clare Moody, Wajid Khan

Motion for a resolution

Paragraph 8

Motion for a resolution

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

Amendment

8. Recognises that planning a successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions; ***notes that there is a limit to how well any CSDP mission can be prepared to protect itself from cyber attacks and that CSDP missions should anticipate operating in a contested cyberspace environment and may find themselves with limited access to information;***

Or. en

Amendment 172

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 8

Motion for a resolution

8. Recognises that planning a

Amendment

8. Recognises that planning a

successful CSDP mission or operation requires substantial cyber defence expertise, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

successful CSDP mission or operation requires substantial cyber defence expertise **and secure IT infrastructure and networks**, both at operational headquarters and within the mission itself, to conduct a thorough threat assessment and provide adequate protection in the field; calls on the EEAS, and on the Member States providing headquarters for CSDP operations, to strengthen their cyber defence expertise to ensure the safety of the EU's missions;

Or. en

Amendment 173
Urmas Paet

Motion for a resolution
Paragraph 8 a (new)

Motion for a resolution

Amendment

8a. Stresses that all CSDP mission and operation planning needs to be accompanied by a thorough assessment of the cyber threat landscape; notes that the threat taxonomy prepared by the European Union Agency for Network and Information Security (ENISA) provides a suitable template for such an assessment; recommends the creation of cyber-resilience assessment capability for CSDP HQs;

Or. en

Amendment 174
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 9

Motion for a resolution

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

Amendment

9. Recognises, in particular, ***that security measures*** (cyber footprints, attack surfaces) ***are a matter for national laws and governments;***

Or. fr

Amendment 175
David McAllister

Motion for a resolution
Subheading 2 a (new)

Motion for a resolution

Recognizes the EDA Training Needs Analysis which has brought up major Cyber Defence skills and competencies shortfalls among decision makers, not only in Member States and welcomes the EDA initiatives on Senior Decision Maker courses within Member States in support of CSDP missions and operations planning;

Amendment

Or. en

Amendment 176
Geoffrey Van Orden

Motion for a resolution
Paragraph 9 a (new)

Motion for a resolution

9a. Recognises that CSDP missions and operations will usually involve Member States that are also NATO Members, and as such, close cooperation

Amendment

with NATO will be required in the planning of such missions;

Or. en

Amendment 177

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Subheading 3

Motion for a resolution

Cyber defence education *and* training

Amendment

Cyber defence education, training *and doctrine-support*

Or. en

Amendment 178

Tunne Kelam

Motion for a resolution

Paragraph 9 a (new)

Motion for a resolution

Amendment

9a. Notes that streamlined EU cyber-defence education and training landscape would significantly mitigate threats and calls on the EU and Member States to increase their cooperation in education, training and exercises;

Or. en

Amendment 179

Geoffrey Van Orden

Motion for a resolution

Paragraph 10

Motion for a resolution

10. **Strongly** supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies **to pay more attention to, and create more possibilities in, the field of cyber defence education;**

Amendment

10. Supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers, **bearing in mind that such interoperability is necessary amongst all NATO allies;** stresses that there is a need for more experts in the cyber defence domain; calls on the military academies **of European nations to include a greater awareness of cyber operations in their training and for more resources to be devoted to specialised cyber operational training;**

Or. en

Amendment 180

Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Patricia Lalonde, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution

Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on **the** military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; **believes however that exchanges for training and education in the field of cyber defence should go beyond this initiative and include military personnel from all ranks and students from all academic institutions with educational programs in cyber security;** stresses that there is a need for more experts in the cyber defence domain; calls on **academic institutions and** military academies to pay more attention to, and create more possibilities in, the field of cyber defence education **and training;**

Amendment 181

Clare Moody, Wajid Khan

Motion for a resolution

Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young *officers*; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young *personnel, of whatever level*; stresses that there is a need for more experts in the cyber defence domain *and*; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education *as well as appropriate funding*;

Amendment 182

Arnaud Danjean

Motion for a resolution

Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports the Military Erasmus initiative aimed at *developing a common strategic culture by* enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment 183

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 10

Motion for a resolution

10. Strongly supports *the Military Erasmus initiative* aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports *common training and exchange initiatives between Member States* aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Or. en

Amendment 184

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 10

Motion for a resolution

10. *Strongly* supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Or. en

Amendment 185
Tunne Kelam

Motion for a resolution
Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; ***stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;***

Amendment

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers;

Or. en

Amendment 186
Urmas Paet

Motion for a resolution
Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers ***and other military personnel***; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education; ***welcomes the introduction by France, with the support of Portugal and Belgium, of an EU pilot module on cyber defence; encourages Member States to foresee the necessary means in their budgets to increase their pool of cyber security experts;***

Amendment 187

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 10

Motion for a resolution

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education;

Amendment

10. Strongly supports the Military Erasmus initiative aimed at enhancing the interoperability of the armed forces of the Member States through an increased exchange of young officers; stresses that there is a need for more experts in the cyber defence domain; calls on the military academies to pay more attention to, and create more possibilities in, the field of cyber defence education, *so that we can increase our cyber talent pool available for CSDP mission's needs*;

Or. en

Amendment 188

Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution

Paragraph 10 a (new)

Motion for a resolution

Amendment

10a. Calls on all Member States to sufficiently and proactively inform, raise awareness and advise companies, schools and citizens about cyber security and the main actual digital threats; welcomes in this regard cyber guides as a tool to guide citizens and organizations towards a better cyber security strategy, to boost cyber security knowledge and improve cyber resilience across the board;

Amendment 189

Tunne Kelam

Motion for a resolution

Paragraph 10 a (new)

Motion for a resolution

Amendment

10a. Stresses that there is a need for more experts in the cyber defence domain; calls on Member States to facilitate cooperation between military and non-military academia to bridge this gap and provide for integrated higher cyber education; calls on the military academies to integrate cyber defence education into their curricula;

Or. en

Amendment 190

Geoffrey Van Orden

Motion for a resolution

Paragraph 10 a (new)

Motion for a resolution

Amendment

10a. Recognises that by their nature, cyber operations are a sensitive domain requiring application of strict 'need to know' principles, while acknowledging the need for a wider, general awareness of the threat;

Or. en

Amendment 191

Hilde Vautmans, Urmas Paet, Ilhan Kyuchyuk, Patricia Lalonde, Javier Nart, María Teresa Giménez Barbat, Jozo Radoš

Motion for a resolution
Paragraph 10 b (new)

Motion for a resolution

Amendment

10b. *Notes that, given the need for more specialised personnel, the focus of the Member States should not only be on recruitment of competent armed forces personnel, but also on the retention of needed specialists;*

Or. en

Amendment 192
Urmaz Paet

Motion for a resolution
Paragraph 11

Motion for a resolution

Amendment

11. *Welcomes the introduction by France, with the support of Portugal and Belgium, of an EU pilot module on cyber defence;*

deleted

Or. en

Amendment 193
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 11

Motion for a resolution

Amendment

11. Welcomes the introduction by France, with the support of Portugal and Belgium, of *an EU* pilot module on cyber defence;

11. Welcomes the introduction by France, with the support of Portugal and Belgium, of *a* pilot module on cyber defence *and points out that resilience stems above all from coordinated national policies;*

Or. fr

Amendment 194
Alojz Peterle

Motion for a resolution
Paragraph 11

Motion for a resolution

11. Welcomes the introduction by France, with the support of Portugal and Belgium, of an EU pilot module on cyber defence;

Amendment

11. Welcomes the introduction by France, with the support of Portugal and Belgium, of an EU pilot module on cyber defence; ***calls for close monitoring of the outcomes and the future implementation of similar programs in other member states in light of positive results;***

Or. en

Amendment 195
Urmas Paet

Motion for a resolution
Paragraph 11 a (new)

Motion for a resolution

11a. Strongly encourages the development of the Cyber Defence Education, Training and Exercise and Evaluation Platform, within the ESDC, with a view to upscaling the training and education opportunities within the Member States;

Or. en

Amendment 196
Bogdan Andrzej Zdrojewski

Motion for a resolution
Paragraph 12

Motion for a resolution

12. Welcomes the implementation – by eleven member states of the Cyber Ranges Federation project – of the first of four cyber defence projects launched under the EDA Pooling and Sharing agenda; calls on the Member States to promote greater mutual availability of virtual cyber defence training and cyber ranges;

Amendment

12. Welcomes the implementation – by eleven member states (*Austria, Belgium, Germany, Estonia, Greece, Finland, Ireland, Latvia, the Netherlands, Portugal and Sweden*) of the Cyber Ranges Federation project – of the first of four cyber defence projects launched under the EDA Pooling and Sharing agenda; ***calls on the other Member States to join this initiative***; calls on the Member States to promote greater mutual availability of virtual cyber defence training and cyber ranges;

Or. pl

Amendment 197

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 12

Motion for a resolution

12. Welcomes the implementation – by eleven member states of the Cyber Ranges Federation project – of the first of four cyber defence projects launched under the EDA Pooling and Sharing agenda; calls on the Member States to promote greater mutual availability of virtual cyber defence training and cyber ranges;

Amendment

12. Welcomes the implementation – by eleven member states of the Cyber Ranges Federation project – of the first of four cyber defence projects launched under the EDA Pooling and Sharing agenda; calls on the Member States to promote greater mutual availability of virtual cyber defence training and cyber ranges; ***in this regard, the role of ENISA and its expertise should be also considered***;

Or. en

Amendment 198

María Teresa Giménez Barbat

Motion for a resolution

Paragraph 12 a (new)

Motion for a resolution

Amendment

12a. *Notes with apprehension the lack of qualified IT professionals working in the field of cybersecurity; urges Member States to invest in education to foster training both in the civil and military sector of IT experts;*

Or. en

Amendment 199

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 13

Motion for a resolution

13. Believes that such initiatives contribute to improving the quality of education in the cyber defence field at EU level, in particular through the creation of wide-ranging technical platforms and the establishment of a community of EU experts;

Amendment

13. Believes that such initiatives contribute to improving the quality of education in the cyber defence field at EU level, in particular through the creation of wide-ranging technical platforms and the establishment of a community of EU experts; *stresses the need to identify weaknesses in the computer systems of both the Member States and the EU institutions; recognises that human error is one of the most frequently identified weaknesses in cybersecurity systems and therefore calls for regular training of both military and civilian personnel working for EU institutions;*

Or. pl

Amendment 200

Clare Moody, Wajid Khan

Motion for a resolution

Paragraph 13

Motion for a resolution

13. Believes that such initiatives contribute to improving the quality of education in the cyber defence field at EU level, in particular through the creation of wide-ranging technical platforms and the establishment of a community of EU experts;

Amendment

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

Or. en

Amendment 201

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 13 a (new)

Motion for a resolution

13a. Encourages more exchanges of situational awareness through table top cyber exercises and coordinating respective capability-development efforts aimed toward the achievement of more interoperability and better prevention and response to future attacks; calls for conducting such projects with NATO allies and other partners with extensive experience in countering cyber attacks, such as Taiwan; in this regard, welcomes the EU involvement in cyber exercises such as CODE (Cyber Offence and Defence Exercise);

Or. en

Amendment 202

Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 14

Motion for a resolution

Amendment

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

deleted

Or. fr

Amendment 203
Ivo Belet

Motion for a resolution
Paragraph 14

Motion for a resolution

Amendment

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

14. Welcomes the establishment of a collaborative platform, the Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises;

Or. en

Amendment 204
Urmas Paet

Motion for a resolution
Paragraph 14

Motion for a resolution

14. ***Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises;*** calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Amendment

14. Calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Or. en

Amendment 205
David McAllister

Motion for a resolution
Paragraph 14

Motion for a resolution

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training ***and*** Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Amendment

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training, Exercise ***and Evaluation*** (***ETEE***) Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform (***CD TEXP***) to support the Cyber Ranges Federation as soon as possible;

Or. en

Amendment 206
Andrea Bocskor

Motion for a resolution
Paragraph 14

Motion for a resolution

14. Strongly encourages the development of a collaborative platform, the planned Cyber **Defence** Education, Training **and** Exercise **Coordination** Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Amendment

14. Strongly encourages the development of a collaborative platform, the planned Cyber Education, Training, Exercise **and** **Evaluation** Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Or. en

Amendment 207
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 14

Motion for a resolution

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible;

Amendment

14. Strongly encourages the development of a collaborative platform, the planned Cyber Defence Education, Training and Exercise Coordination Platform, within the ESDC with a view to facilitating the pooling and sharing of training and exercises; calls on the EDA to launch the Cyber Defence Training and Exercise Coordination Platform to support the Cyber Ranges Federation as soon as possible ***with a focus towards strengthening cooperation on harmonized requirements, fostering cyber defence research and technology innovations, and collectively assisting third countries in building their capacities to create resilience in cyber security;***

Or. en

Amendment 208

Ivo Belet

Motion for a resolution

Paragraph 14 a (new)

Motion for a resolution

Amendment

14a. Calls on the Commission and the Member States to complement these initiatives with a dedicated European Centre of Excellence for Cyber Defence Training to provide expert training for the most promising recruits, in support of the participating Member States' cyber training;

Or. en

Amendment 209

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 14 a (new)

Motion for a resolution

Amendment

14a. Recalls the need of developing more joint exercises between EU armed forces, in order to develop operational readiness, common procedures and standards to comprehensively face different cyber threats;

Or. en

Amendment 210

Tunne Kelam

Motion for a resolution

Paragraph 14 a (new)

Motion for a resolution

Amendment

14a. *Reminds that resilient cyber space requires impeccable cyber hygiene; calls on all public and private stakeholders to conduct regular cyber hygiene trainings for all members of their staff;*

Or. en

Amendment 211
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 14 b (new)

Motion for a resolution

Amendment

14b. *Recommends to increase the exchange of expertise and lessons learned between armed forces, police forces and other state bodies active in Member States and involved in the fight against cyber threats;*

Or. en

Amendment 212
James Carver

Motion for a resolution
Subheading 4

Motion for a resolution

Amendment

EU-NATO cooperation on cyber defence

deleted

Or. en

Amendment 213
Tunne Kelam

Motion for a resolution
Paragraph 14 b (new)

Motion for a resolution

Amendment

14b. *Reiterates that, on the basis of their common values and strategic interests, the EU and NATO have a special responsibility and capacity to address the increasing cyber security and cyber defence challenges more efficiently and in close cooperation by looking for possible complementarities, without duplication and with respect for their respective responsibilities;*

Or. en

Amendment 214
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Paragraph 14 a (new)

Motion for a resolution

Amendment

14a. *Calls on the Council to consider, working with other relevant EU institutions and structures, ways to provide, at the earliest convenience possible, Union-level support for integrating the cyber domain into Member States military doctrines, in a harmonized manner, and in close cooperation with NATO;*

Or. en

Amendment 215
James Carver

Motion for a resolution
Paragraph 15

Motion for a resolution

Amendment

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

deleted

Or. en

Amendment 216

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 15

Motion for a resolution

Amendment

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy ***which aims to increase the training capabilities on IT and cyber systems, both software and hardware regarding cyber defence, including a dialogue with NATO on the possibility of EU joining the Centre as a party to increase complementarity and collaboration for the good of citizens in both the EU and NATO***; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Or. en

Amendment 217
David McAllister

Motion for a resolution
Paragraph 15

Motion for a resolution

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Amendment

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence (**CCD COE**) and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Or. en

Amendment 218
Marietje Schaake, Urmas Paet, Javier Nart, Patricia Lalonde, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution
Paragraph 15

Motion for a resolution

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Amendment

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats; ***urges all relevant institutions to regularly meet to discuss their activities in order to avoid overlaps and encourage a coordinated approach towards cyber defence;***

Or. en

Amendment 219
Victor Boştinaru

Motion for a resolution
Paragraph 15

Motion for a resolution

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Amendment

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats; ***believes that it is crucial to stimulate the exchange of cyber threat intelligence data, based on mutual trust, between EU Member States and with NATO;***

Or. en

Amendment 220
Arnaud Danjean

Motion for a resolution
Paragraph 15

Motion for a resolution

15. Calls for identifying new initiatives to further cooperation between EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Amendment

15. Calls for ***the implementation in practice of measures already committed to;*** calls for identifying new initiatives to further cooperation between ***the*** EU and NATO, taking into account as well the possibilities of cooperating within the NATO Cooperative Cyber Defence Centre of Excellence and the NATO Communications and Information (NCI) Academy; welcomes the recent creation of the European Centre of Excellence for Countering Hybrid Threats;

Amendment 221

James Carver

Motion for a resolution

Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

deleted

Or. en

Amendment 222

Ana Gomes

Motion for a resolution

Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is **vital** in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is **important and useful** in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Or. en

Amendment 223
Victor Boştinaru

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence ***to prevent, detect and deter cyber attacks***; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint ***exercises and*** training for cyber defence staff;

Or. en

Amendment 224
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff ***and EU participation in NATO smart defence projects***;

Or. en

Amendment 225
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for *civilian and military* cyber defence staff;

Or. en

Amendment 226

Marietje Schaake, Urmas Paet, Javier Nart, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff; *considers it vital that the EU and NATO step up the sharing of intelligence in order to enable the formal attribution of cyberattacks and consequently enable the imposition of restrictive sanctions to those responsible for cyberattacks;*

Or. en

Amendment 227
Urmas Paet

Motion for a resolution
Paragraph 16

Motion for a resolution

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff;

Amendment

16. Is convinced that increased cooperation between EU and NATO is vital in the area of cyber defence; calls, therefore, on both organisations to increase their operational cooperation and coordination, and to expand their joint capacity-building efforts, in particular joint training for cyber defence staff; ***urges both organisations to cooperate more closely also on the cyber aspects of crisis management;***

Or. en

Amendment 228
Urmas Paet

Motion for a resolution
Paragraph 16 a (new)

Motion for a resolution

Amendment

16a. Welcomes the exchange of concepts to integrate cyber defence requirements and standards into planning and conduct of missions and operations to foster interoperability and expresses the hope that this will be followed up by more operational cooperation on ensuring the cyber defence of respective missions and synchronisation of operational approaches;

Or. en

Amendment 229
James Carver

Motion for a resolution
Paragraph 17

Motion for a resolution

Amendment

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

deleted

Or. en

Amendment 230
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 17

Motion for a resolution

Amendment

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support, **shared threat assessments, personnel acquisition** and the sharing of best practices **in order to respond to threats in real time**; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

Or. en

Amendment 231
Raffaele Fitto

Motion for a resolution
Paragraph 17

Motion for a resolution

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

Amendment

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices, ***nationally and within NATO***; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

Or. it

Amendment 232
Urmas Paet

Motion for a resolution
Paragraph 17

Motion for a resolution

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (***CERT***) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between ***CERTs*** and to work towards increasing the level of trust;

Amendment

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (***CERT-EU***) and the NATO Computer Incident Response Capability (***NCIRC***) aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between ***CERT-EU and NCIRC*** and to work towards increasing the level of trust;

Or. en

Amendment 233
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 17

Motion for a resolution

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;

Amendment

17. Welcomes the arrangement between the EU's Computer Emergency Response Team (CERT) and the NATO Computer Incident Response Capability aimed at facilitating the exchange of information, logistical support and the sharing of best practices; stresses that it is important to encourage information exchanges between CERTs and to work towards increasing the level of trust;
believes that there is an assumption that information held by CERT could be of use to cyber defence research and NATO and that this information should be shared providing full conformity with EU data protection legislation is applied;

Or. en

Amendment 234
James Carver

Motion for a resolution
Paragraph 18

Motion for a resolution

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

Amendment

deleted

Or. en

Amendment 235

James Carver

Motion for a resolution

Paragraph 19

Motion for a resolution

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

Amendment

deleted

Or. en

Amendment 236

Georgios Epitideios

Motion for a resolution

Paragraph 19

Motion for a resolution

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

Amendment

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

Or. el

Amendment 237

James Carver

Motion for a resolution
Paragraph 20

Motion for a resolution

20. *Notes that there is substantial scope for a more ambitious and concrete cyber defence cooperation programme that goes beyond the conceptual level of cooperation in the context of specific operations; urges both organisations to present more ambitious proposals for the next review of the implementation of the Joint Statement;*

Amendment

deleted

Or. en

Amendment 238
Arnaud Danjean

Motion for a resolution
Paragraph 20

Motion for a resolution

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

Amendment

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

Or. fr

Amendment 239
Andrea Bocskor

Motion for a resolution
Paragraph 20

Motion for a resolution

20. Notes that there is substantial scope for a more ambitious and concrete cyber defence cooperation programme that goes beyond the conceptual level of cooperation in the context of specific operations; urges both organisations to present more ambitious proposals for the next review of the implementation of the Joint **Statement**;

Amendment

20. Notes that there is substantial scope for a more ambitious and concrete cyber defence cooperation programme that goes beyond the conceptual level of cooperation in the context of specific operations; urges both organisations to present more ambitious proposals for the next review of the implementation of the Joint **Declaration**;

Or. en

Amendment 240

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 20 a (new)

Motion for a resolution

20a. Welcomes the NATO Industry Cyber Partnership (NICP) established in 2014, and seeks EU engagement in cooperative NICP efforts to connect NATO-EU cooperation with industry leaders specialized in cyber technologies to advance cyber security through continued collaboration with particular focus towards: trainings, exercises, and education for both NATO, EU and industry representatives, EU and industry inclusion in NATO Smart Defence projects, collaborative information sharing and best practices for preparedness and recovery between NATO, EU and industry, pursuit of jointly developed capabilities for cyber defence, and to ensure collaborative responses to cyber incidents when and where appropriate;

Or. en

Amendment 241

Marietje Schaake, Urmas Paet, Javier Nart, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Paragraph 20 a (new)

Motion for a resolution

Amendment

20a. Notes the ongoing work on the Proposal for a Regulation revising ENISA Regulation (No 526/2013) and laying down a European ICT security certification and labelling framework; calls on ENISA to sign an agreement with NATO to increase their practical cooperation, including the sharing of information and participation in cyber defence exercises;

Or. en

Amendment 242

Tunne Kelam

Motion for a resolution

Paragraph 20 a (new)

Motion for a resolution

Amendment

20a. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

Or. en

Amendment 243

Tunne Kelam

Motion for a resolution

Paragraph 20 b (new)

Motion for a resolution

Amendment

20b. *Calls on a clear proactive approach towards cyber security and cyber defence and the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally;*

Or. en

Amendment 244
Urmas Paet

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts *failed to adopt a* consensus report; recalls, *however*, that international law applies to cyberspace and that the *2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards* the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Amendment

21. Regrets that, after several months of negotiations, the *2016-2017 UN Group of Governmental Experts (UNGGE) was not able to produce a new* consensus report; recalls that *as recognized by the 2013 report*, international law applies to cyberspace and that the *2015 UNGGE report lists a set of norms of responsible state behaviour including* the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Or. en

Amendment 245
Andrea Bocskor

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies to cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the *prohibition for* states *to* conduct or knowingly support cyber activities contrary to their obligations under international *rules*;

Amendment

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that *existing* international law applies to cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the *expectation that* states *should not* conduct or knowingly support cyber activities contrary to their obligations under international *law*;

Or. en

Amendment 246
Arnaud Danjean

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies to cyberspace *and* that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Amendment

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law, *and the United Nations Charter in particular*, applies to cyberspace, that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Or. fr

Amendment 247
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies *to* cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Amendment

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies *in* cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Or. en

Amendment 248
Tunne Kelam

Motion for a resolution
Paragraph 21

Motion for a resolution

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies to cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules;

Amendment

21. Regrets that, after several months of negotiations, the UN Group of Governmental Experts failed to adopt a consensus report; recalls, however, that international law applies to cyberspace and that the 2013 and 2015 UNGGE reports still provide relevant guidelines, in particular as regards the prohibition for states to conduct or knowingly support cyber activities contrary to their obligations under international rules; ***calls on the EU to assume a leading role in the ongoing and future debates on international norms in cyberspace;***

Or. en

Amendment 249

Marietje Schaake, Urmas Paet, Javier Nart, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution

Paragraph 21 a (new)

Motion for a resolution

Amendment

21a. Notes in this regard the importance of article 2(4) of the UN Charter States, which calls on states to refrain from the threat or use of force against the political independence of any state; believes that this includes a prohibition to pursue or knowingly support coercive cyber operations intended to disrupt the technical infrastructure essential to the conduct of official participative procedures in another state, including elections and referenda;

Or. en

Amendment 250

Urmas Paet

Motion for a resolution

Paragraph 22

Motion for a resolution

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 **in this context** as an excellent basis for a debate **on how** international law **applies** to cyberspace; notes that it is now time for the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

22. Notes the relevance of the Tallinn Manual 2.0 as an excellent basis for a debate **and offering analysis how existing** international law **can be applied** to cyberspace; notes that it is now time for the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

Or. en

Amendment 251

Arnaud Danjean

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Notes the relevance of the Tallinn Manual 2.0 in this context as ***an excellent*** basis for a debate on how international law applies to cyberspace; notes that it is now time for the Member States to start analysing ***and applying*** what the experts have stated in the Tallinn Manual;

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 in this context as ***a*** basis for a debate on how international law applies to cyberspace; notes that it is now time for the Member States to start analysing what the experts have stated in the Tallinn Manual;

Or. fr

Amendment 252
Bogdan Andrzej Zdrojewski

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace; ***notes that it is now time for*** the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace; ***calls on*** the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

Or. pl

Amendment 253
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law

applies *to* cyberspace; notes that it is now time for the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

applies *in* cyberspace; notes that it is now time for the Member States to start analysing and *consider* applying what the experts have stated in the Tallinn Manual *in order to build international consensus on how to apply international law in cyberspace and to agree further voluntary norms of international behaviour*;

Or. en

Amendment 254
Geoffrey Van Orden

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace; notes that it is now time for the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace, *both during peacetime and periods of armed conflict*; notes that it is now time for the Member States to start analysing and applying what the experts have stated in the Tallinn Manual;

Or. en

Amendment 255
Marietje Schaake, Urmas Paet, Javier Nart, Patricia Lalonde, Jozo Radoš, María Teresa Giménez Barbat

Motion for a resolution
Paragraph 22

Motion for a resolution

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace; notes that it is now time for the Member States to start

Amendment

22. Notes the relevance of the Tallinn Manual 2.0 in this context as an excellent basis for a debate on how international law applies to cyberspace; notes that it is now time for the Member States to start

analysing and applying what the experts have stated in the Tallinn Manual;

analysing and applying what the experts have stated in the Tallinn Manual; ***notes in particular that any offensive use of cyber capabilities should be based on international law;***

Or. en

Amendment 256
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to ***an*** open, free, stable and ***secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means;*** calls on the Member States to promote ***further implementation of the common and comprehensive EU approach to cyber diplomacy;*** strongly supports the development of voluntary, ***non-binding*** norms ***of responsible state*** behaviour in cyberspace;

Amendment

23. Confirms its full commitment to ***a secure cyberspace, which means Member States need control of the hardware and software linked to cyberspace so that it is open, free, stable at EU level and not subject to disputes and manipulation from outside forces;*** calls on the Member States to promote ***a collaborative*** approach; strongly supports the development, ***and establishment at national level,*** of voluntary norms ***enabling control over expertise so that EU States behave responsibly*** in cyberspace;

Or. fr

Amendment 257
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are

settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the **development of** voluntary, non-binding norms of responsible state behaviour in cyberspace;

settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy **and existing cyber norms**; strongly supports the **implementation of the 2015 UNGGE report** voluntary, non-binding norms of responsible state behaviour in cyberspace, **with eventual pursuit of a binding international framework**;

Or. en

Amendment 258
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy **and draw up, together with NATO, EU-level criteria and definitions of what constitutes a cyber attack so as to improve the EU's ability to quickly come to a common position following an internationally wrongful act in the form of a cyber attack**; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Or. en

Amendment 259
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace, ***as well as the creation of an attribution organization within an international agreement to address the issue of the attribution of an attack;***

Or. en

Amendment 260
Ana Gomes

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means ***on the basis of the UN Charter and principles of international law;*** calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary,

cyberspace;

non-binding norms of responsible state behaviour in cyberspace, ***encompassing respect for privacy and fundamental rights of citizens***;

Or. en

Amendment 261
David McAllister

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace, ***in conjunction with the creation of regional confidence-building measures***;

Or. en

Amendment 262
Georgios Epitideios

Motion for a resolution
Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which ***respects*** the core values of democracy, human rights and the rule of

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which ***will allow States to promote their interests, but will respect*** the core values

law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Or. el

Amendment 263 **Urmas Paet**

Motion for a resolution **Paragraph 23**

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development *and implementation* of voluntary, non-binding norms of responsible state behaviour in cyberspace *and regional confidence building measures*;

Or. en

Amendment 264 **Marietje Schaake, Urmas Paet, Javier Nart, Patricia Lalonde, Nadja Hirsch, Jozo Radoš, María Teresa Giménez Barbat**

Motion for a resolution **Paragraph 23**

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace; ***Supports in this context the work of the Global Commission on the Stability of Cyberspace to develop proposals for norms and policies to enhance international security and stability and guide responsible state and non-state behaviour in cyberspace; endorses the proposal that state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace;***

Or. en

Amendment 265

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 23

Motion for a resolution

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further

Amendment

23. Confirms its full commitment to an open, free, stable and secure cyberspace, which respects the core values of democracy, human rights and the rule of law, and where international disputes are settled by peaceful means; calls on the Member States to promote further

implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace;

implementation of the common and comprehensive EU approach to cyber diplomacy; strongly supports the development of voluntary, non-binding norms of responsible state behaviour in cyberspace; *notes that a large proportion of cyber-attacks against states originate from private actors, and therefore calls for an analysis of the possibilities for legal action against such actors;*

Or. pl

Amendment 266

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 23 a (new)

Motion for a resolution

Amendment

23a. Stresses the need to strengthen cyber-diplomacy as a cross-sectional task in the EU's foreign policy and its capacities and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as lead to the reaching of consensus on the rules, norms and enforcement measures in cyberspace globally;

Or. en

Amendment 267

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 23 a (new)

Motion for a resolution

Amendment

23a. Recognizes that a majority of the technological infrastructure is owned or operated by the private sector, and therefore, that close cooperation,

consultation, and inclusion of the private sector and civil society groups through multi-stakeholder dialogue is essential to ensuring an open, free, stable and secure cyberspace;

Or. en

Amendment 268

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 24

Motion for a resolution

24. **Recognises** that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement multilateral efforts;

Amendment

24. **Regrets** that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement multilateral efforts;

Or. pl

Amendment 269

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 24

Motion for a resolution

24. Recognises that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement **multilateral** efforts;

Amendment

24. Recognises that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement **multi-stakeholder** efforts;

Or. en

Amendment 270

Raffaele Fitto

Motion for a resolution

Paragraph 24

Motion for a resolution

24. Recognises that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement multilateral efforts;

Amendment

24. Recognises that, owing to difficulties in enforcement, bilateral agreements between states do not always bring expected results; considers, therefore, that building coalitions within groups of like-minded countries willing to generate consensus constitutes an effective way to complement multilateral efforts; ***stresses the importance of the role of local authorities in the process of technological innovation and data sharing in order to step up the fight against crime and terrorist activities;***

Or. it

Amendment 271

Urmas Paet

Motion for a resolution

Paragraph 24 a (new)

Motion for a resolution

Amendment

24a. Welcomes the adoption by the Council of the framework for joint EU diplomatic responses to malicious cyber activities, the so-called EU Cyber Diplomacy Toolbox; supports the possibility for the EU to take restrictive measures against adversaries attacking its Member States in cyberspace, including a possible imposition of sanctions;

Or. en

Amendment 272
Geoffrey Van Orden

Motion for a resolution
Paragraph 25

Motion for a resolution

Amendment

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally; *deleted*

Or. en

Amendment 273
Tunne Kelam

Motion for a resolution
Paragraph 25

Motion for a resolution

Amendment

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally; *deleted*

Or. en

Amendment 274
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 25

Motion for a resolution

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally;

Amendment

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally, ***eventually leading to a binding non-proliferation agreement;***

Or. en

Amendment 275

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 25

Motion for a resolution

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally;

Amendment

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally; ***reminds that it is of utmost importance to establish and enforce international norms and values such as the UN Charter also in cyberspace;***

Or. en

Amendment 276

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 25

Motion for a resolution

25. Calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally;

Amendment

25. *Also* calls on the strengthening of the EU's cyber diplomacy capacity and instruments across the board, so that they can effectively reinforce the EU's norms and values, as well as help the parties concerned to reach consensus on rules, norms and enforcement measures in cyberspace globally;

Or. en

Amendment 277

Clare Moody, Wajid Khan

Motion for a resolution

Paragraph 25 a (new)

Motion for a resolution

25a. Considers that cyber attacks such as NotPetya and WannaCry are either state directed or take place with the knowledge of the state and its approval; notes that these cyber attacks which cause serious and lasting economic damage as well as being a threat to life, are clear breaches of international law and legal norms; believes therefore that the case of NotPetya and WannaCry represent breaches of international law for which the Russian Federation and North Korea respectively are culpable and should face commensurate and appropriate responses from the EU and NATO;

Or. en

Amendment 278

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 25 a (new)

Motion for a resolution

Amendment

25a. *Promote within Europol's Cybercrime Centre a focal point for law enforcement divisions and government agencies dedicated to cybercrime whose primary responsibility would be to manage the defence of both the dot-eu domains and critical infrastructure of the EU networks during an attack; emphasises that such a focal point should also be mandated to exchange information and provide nations with assistance;*

Or. en

Amendment 279
Victor Boştinaru

Motion for a resolution
Paragraph 25 a (new)

Motion for a resolution

Amendment

25a. *Emphasises the importance of the development of norms regarding privacy and security , regarding encryption , hate speech, disinformation and terrorism threats;*

Or. en

Amendment 280
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 25 b (new)

Motion for a resolution

Amendment

25b. *Recommends that EU Member States embrace an obligation to assist a fellow Member State under cyber attack*

*and to ensure national cyber
accountability in close cooperation with
NATO;*

Or. en

Amendment 281
Geoffrey Van Orden

Motion for a resolution
Paragraph 26

Motion for a resolution

Amendment

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

deleted

Or. en

Amendment 282
Indrek Tarand
on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 26

Motion for a resolution

Amendment

26. Calls on *all* stakeholders to *reinforce* knowledge transfer partnerships, *implement* appropriate business models and *develop* trust between *companies and defence and civilian end-users*, as well as *to improve* the transfer of academic knowledge into practical solutions, *in order to create synergies and port*

26. Calls on *the Member States and the Commission to ensure a clear framework for cooperation of all relevant stakeholders; believes that also* knowledge transfer partnerships, appropriate business models and *the further development of* trust between *different stakeholders need to be considered*, as well as *the*

solutions between the civilian and military markets – in essence a single market for cybersecurity;

improvement of the transfer of academic knowledge into practical solutions; believes that there is no need for direct subsidies at EU level to companies in the cybersecurity market;

Or. en

Amendment 283
Ana Gomes

Motion for a resolution
Paragraph 26

Motion for a resolution

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military *markets – in essence a single market for cybersecurity;*

Amendment

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military *realms, based on transparent procedures and in respect of EU and international law, with the view of preserving and strengthening the EU's strategic autonomy;*

Or. en

Amendment 284
Victor Boştinaru

Motion for a resolution
Paragraph 26

Motion for a resolution

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as

Amendment

26. *Emphasises that the dual- use nature of cyber-technologies would need to integrate cybersecurity into the Common Defence and Security Policy and to promote synergies between military ad*

to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

civilian efforts; Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

Or. en

Amendment 285
Urmas Paet

Motion for a resolution
Paragraph 26

Motion for a resolution

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

Amendment

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity ***and cyber security products***;

Or. en

Amendment 286
Tunne Kelam

Motion for a resolution
Paragraph 26

Motion for a resolution

26. Calls on all stakeholders to

Amendment

26. Calls on all stakeholders to

reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a *European* single market for cybersecurity;

Or. en

Amendment 287

Clare Moody, Wajid Khan

Motion for a resolution

Paragraph 26

Motion for a resolution

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity;

Amendment

26. Calls on all stakeholders to reinforce knowledge transfer partnerships, implement appropriate business models and develop trust between companies and defence and civilian end-users, as well as to improve the transfer of academic knowledge into practical solutions, in order to create synergies and port solutions between the civilian and military markets – in essence a single market for cybersecurity; *notes the pivotal role that private cybersecurity firms play in early warning and attribution of cyber attacks;*

Or. en

Amendment 288

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the **EU and the** Member States to give more practical support to **the EU cyber-security industry**, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), **and to** promote closer cooperation with university research organisations **and large players with a view to reducing** dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU; **notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;**

Amendment

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the Member States to give more practical support to **relevant economic actors**, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), promote closer cooperation with university research organisations, **to reduce** dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU; **urges the Council to adopt a general approach on the Recast of the Dual-Use Regulation without further delay in order to allow an already much delayed start of inter-institutional negotiations on stricter rules for the export of cyber surveillance and security technology to third countries; underlines that unregulated exports from EU Member States of such cyber technology to third countries potentially endangers the Union's security;**

Or. en

Amendment 289
Geoffrey Van Orden

Motion for a resolution
Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to **the EU** cyber-security **industry**, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer

Amendment

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to **European** cyber-security **industries**, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer

cooperation with university research organisations and large players *with a view to reducing dependencies on cyber security products form external sources and to creating a strategic supply chain inside the EU*; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

cooperation with university research organisations and large players;

Or. en

Amendment 290

Ana Gomes

Motion for a resolution

Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products form external sources *and to creating a strategic supply chain inside the EU*; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Amendment

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products form external sources, creating a strategic supply chain inside *the EU and enhancing the strategic autonomy of the EU*; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Or. en

Amendment 291

Anna Elżbieta Fotyga

Motion for a resolution

Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the **EU** cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to **reducing dependencies on cyber security products form external sources and to** creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Amendment

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the **European** cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to creating a strategic supply chain inside the EU **whilst recognizing the leading role of the transatlantic cooperation in this regard**; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Or. en

Amendment 292

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 27

Motion for a resolution

27. **Recalls** the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products form external sources and to

Amendment

27. **Strongly emphasises** the **crucial** importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products

creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

form external sources and to creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Or. pl

Amendment 293

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products form external sources and to creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the *future* EDF and other instruments under the MFF;

Amendment

27. Recalls the importance of R&D, in particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products form external sources and to creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the EDF and other instruments under the MFF;

Or. en

Amendment 294

Tunne Kelam

Motion for a resolution

Paragraph 27

Motion for a resolution

27. Recalls the importance of R&D, in

Amendment

27. Recalls the importance of R&D, in

particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry, in particular SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

particular in the light of the high-level security requirements in the defence market; urges the EU and the Member States to give more practical support to the EU cyber-security industry **and reduce bureaucratic burdens**, in particular **for** SMEs and start-ups (key sources of innovative solutions in the area of cyber defence), and to promote closer cooperation with university research organisations and large players with a view to reducing dependencies on cyber security products from external sources and to creating a strategic supply chain inside the EU; notes, in this context, the valuable contribution that can be made by the future EDF and other instruments under the MFF;

Or. en

Amendment 295

Urmas Paet

Motion for a resolution

Paragraph 27 a (new)

Motion for a resolution

Amendment

27a. Encourages the Commission to integrate cyber defence elements into the Network of European Cybersecurity Competence and Research Centers, also in view of providing sufficient resources to dual use cyber capabilities and technologies within the next Multiannual Financial Framework;

Or. en

Amendment 296

Arnaud Danjean

Motion for a resolution

Paragraph 28

Motion for a resolution

Amendment

28. *Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;*

deleted

Or. fr

Amendment 297

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 28

Motion for a resolution

Amendment

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task *that* should *form* part of the *remit of national cyber commands*; stresses that this will require a level of trust, and the closest possible cooperation, between *military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes*;

28. Notes that the protection of civilian critical infrastructure assets, *in particular information systems and associated data*, is becoming a vital defence task *which* should *be* part of the *government's respective duty of care*; stresses that this will require a level of trust, and the closest possible cooperation between all stakeholders;

Or. en

Amendment 298

Patricia Lalonde

Motion for a resolution

Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital *defence* task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital task *for Member States, particularly for the authorities in charge of information systems security, and that this task should either form part of the remit of national cyber commands or the remit of said authorities*; stresses that this will require a level of trust, and the closest possible cooperation, between military actors, *cyber defence agencies, all other authorities concerned*, and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Or. fr

Amendment 299
Fabio Massimo Castaldo

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, *and the closest possible* cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust *and* cooperation between military actors and the affected industries, *by clearly defining duties, roles and responsibilities of civilian and military actors* and urges all stakeholders to take this into account in their planning processes;

Or. en

Amendment 300
Urmaz Paet

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of **civilian** critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of **public and other civil** critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Or. en

Amendment 301
Bogdan Andrzej Zdrojewski

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is **becoming** a vital defence task that **should** form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is a vital defence task that **must** form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Or. pl

Amendment 302
Tunne Kelam

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is **becoming** a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Or. en

Amendment 303
Ana Gomes

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national **and European** cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Or. en

Amendment 304
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 28

Motion for a resolution

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes;

Amendment

28. Notes that the protection of civilian critical infrastructure assets is becoming a vital defence task that should form part of the remit of national cyber commands; stresses that this will require a level of trust, and the closest possible cooperation, between military actors and the affected industries, and urges all stakeholders to take this into account in their planning processes; ***urges more cross-border cooperation, whilst fully respecting EU data protection legislation, on law enforcement related to taking down malicious cyber activity;***

Or. en

Amendment 305

Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution

Paragraph 28 a (new)

Motion for a resolution

Amendment

28a. Calls on all Member States to focus national cyber security strategies on the protection of information systems and associated data and to consider the protection of this critical infrastructure as part of their respective duty of care; urges the Member States to adopt and implement strategies, guidelines and instruments that provide reasonable levels of protection against reasonably identifiable levels of threats, with costs and burdens of the protection proportionate to the probable damage to the parties concerned; calls on Member States to take appropriate steps to oblige legal persons under their jurisdictions to protect personal data under their care;

Amendment 306

Urmas Paet

Motion for a resolution

Paragraph 28 a (new)

Motion for a resolution

Amendment

28a. Encourages close cooperation between EU agencies such as EDA, ENISA, the European Cybercrime Centre in a cross-sectoral approach in order to promote synergies and avoid overlapping;

Or. en

Amendment 307

Jean-Luc Schaffhauser

Motion for a resolution

Paragraph 29

Motion for a resolution

Amendment

29. Calls on the EEAS and EDA, in close cooperation with the Commission, to take work forward on the update of the EU Cyber Defence Policy Framework to ensure that it remains fit for purpose as the relevant policy mechanism for achieving the EU's cyber defence objectives;

29. Points out that neither the EEAS, the EDA nor the Commission have any legitimacy other than that which the Member States decide to grant them so they may better coordinate their actions, and that the Member States still retain full responsibility for all of their security and defence policies, these being policies that on principle cannot be delegated;

Or. fr

Amendment 308

Arne Lietz, Eugen Freund

Motion for a resolution

Paragraph 29

Motion for a resolution

29. Calls on the **EEAS and EDA, in close cooperation with the Commission, to take work forward on the** update of the EU Cyber Defence Policy Framework to ensure that it remains fit for purpose as the relevant policy mechanism for achieving the EU's cyber defence objectives;

Amendment

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

Or. en

Amendment 309

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 29

Motion for a resolution

29. Calls on the EEAS and EDA, in close cooperation with the Commission, to **take work forward on the update of** the EU Cyber Defence Policy Framework to **ensure that it remains** fit for purpose as the relevant policy mechanism for achieving the EU's cyber defence objectives;

Amendment

29. Calls on the EEAS and EDA, in close cooperation with the Commission, to **revise** the EU Cyber Defence Policy Framework to **better define the roles and responsibilities between the EU institutions, agencies and member states, within a common governance framework, in order to be** fit for purpose as the relevant policy **support** mechanism for achieving the EU's cyber defence objectives;

Or. en

Amendment 310

Antonio López-Istúriz White

Motion for a resolution
Paragraph 30

Motion for a resolution

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries;

Amendment

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries; ***recalls that when Europe's surroundings are vulnerable, then Europe is vulnerable too; notes that increasing server capacity and cyber in the Southern and Eastern Neighbourhood might be used for deploying cyber-attacks against private actors in Europe, Member States, and the Union itself; emphasizes, moreover, an increasing use of online platforms will give greater access for adept asymmetric powers to feed rivalling, polarizing or even extremist narratives to the detriment of the European Union's relations or reputation in these countries, as seen in North America and Europe;***

Or. en

Amendment 311
Indrek Tarand

on behalf of the Verts/ALE Group

Motion for a resolution
Paragraph 30

Motion for a resolution

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries;

Amendment

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries; ***calls on Member States and the Commission to focus in particular on relevant European companies and their obligations to protect data of third country citizens well and including the provision***

of resilient information and data infrastructure especially since the primary consideration for hardware purchases in developing countries is often the affordability of the hardware, not its security profile;

Or. en

Amendment 312

Ana Gomes

Motion for a resolution

Paragraph 30

Motion for a resolution

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries;

Amendment

30. Calls for cyber security capacity building through development cooperation, taking into account that in the coming years millions of new internet users will go online, most of them in developing countries; *taking also into account that cyber crimes are increasing in the world and that illicitly financial flows moves instantly around the globe through cyberspace; taking additionally into account that corruption, tax fraud and tax evasion and other economic and financial crimes are cyber-enabled and often imply a degree of capture of governments and political establishments;*

Or. en

Amendment 313

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 30

Motion for a resolution

30. Calls for cyber security capacity building through development cooperation,

Amendment

30. Calls for cyber security capacity building through development cooperation,

taking into account that in the coming years millions of new internet users will go online, most of them in developing countries;

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

Or. en

Amendment 314
Ana Gomes

Motion for a resolution
Paragraph 30 – subparagraph 1 (new)

Motion for a resolution

Amendment

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

Or. en

Amendment 315
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 30 a (new)

Motion for a resolution

Amendment

30a. Notes that cyber attacks such as NotPetya spread quickly, thereby causing indiscriminate damage, unless there is widespread resilience globally; believes that cyber defence training and education

should form part of the EU's external action and that building cyber resilience in third countries contributes to international peace and security ultimately making European citizens safer;

Or. en

Amendment 316
Eva Kaili, Nikos Androulakis

Motion for a resolution
Paragraph 30 a (new)

Motion for a resolution

Amendment

30a. Calls for further coordination between the EEAS, NATO and the European Commission on civil threats that could destabilize political systems and have greater implications, such as the dissemination of false information, most notably in cases where there are hubs of such activity such as the city of Veles in the Former Yugoslav Republic of Macedonia;

Or. en

Amendment 317
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 31

Motion for a resolution

Amendment

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

deleted

Amendment 318
Georgios Epitideios

Motion for a resolution
Paragraph 31

Motion for a resolution

Amendment

31. *Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;*

deleted

Or. el

Amendment 319
Geoffrey Van Orden

Motion for a resolution
Paragraph 31

Motion for a resolution

Amendment

31. *Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;*

deleted

Or. en

Amendment 320
Tunne Kelam

Motion for a resolution
Paragraph 31

Motion for a resolution

Amendment

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

deleted

Or. en

Amendment 321

Fabio Massimo Castaldo

Motion for a resolution

Paragraph 31

Motion for a resolution

Amendment

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

31. Calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, *police forces* and other credible partners;

Or. en

Amendment 322

Ana Gomes

Motion for a resolution

Paragraph 31

Motion for a resolution

Amendment

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States

31. Emphasises the need to mainstream cyber defence *capabilities* into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United

and other credible partners;

Nations, the United States and other credible partners;

Or. en

Amendment 323

David McAllister

Motion for a resolution

Paragraph 31

Motion for a resolution

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other *credible* partners;

Amendment

31. Emphasises the need to mainstream cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other *strategic* partners;

Or. en

Amendment 324

Bogdan Andrzej Zdrojewski

Motion for a resolution

Paragraph 31

Motion for a resolution

31. *Emphasises the need to mainstream* cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

Amendment

31. *Calls for the mainstreaming of* cyber defence into external action and common foreign and security policy, and calls for closer coordination on cyber defence between the Member States, the EU institutions, NATO, the United States and other credible partners;

Or. pl

Amendment 325

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Subheading 6 a (new)

Motion for a resolution

Amendment

Institutional reinforcement

Or. en

Amendment 326
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Paragraph 31 a (new)

Motion for a resolution

Amendment

31a. Calls on the Member States to have more ambitious cooperation in the cyber domain within PESCO; suggests to Member States to launch a new PESCO cyber cooperative programme in order to support quick and effective planning, command and control of present and future EU operations and missions; notes that this should lead to better coordination of operational capacities in cyberspace and may lead to the development of a common cyber defence command when the European Council so decides;

Or. en

Amendment 327
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Paragraph 31 b (new)

Motion for a resolution

Amendment

31b. Repeats its call on the Member States and the VP/HR to present an EU White Book on Security and Defence;

calls on the Member States and the VP/HR to make cyber defence and deterrence a corner stone of the White Book covering both the protection of the cyber domain for operations laid down in article 43 and common defence laid down in Article 42(7) TEU;

Or. en

Amendment 328

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 31 c (new)

Motion for a resolution

Amendment

31c. Notes that the new PESCO cyber cooperative programme should be led by both high-ranking military and civilian staff from each member state, on a rotating basis, and be accountable to the EU ministers of defence in the PESCO format and the VP/HR, in order to foster the principles of trust among member states and EU institutions and agencies concerning the sharing of information and intelligence;

Or. en

Amendment 329

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 31 d (new)

Motion for a resolution

Amendment

31d. Repeats its call to create an EU Council on Defence built out of the existing EDA ministerial Steering Board and the PESCO format of the EU ministers of defence, in order to

*guarantee prioritization,
operationalization of resources and
effective cooperation and integration
among Member States;*

Or. en

Amendment 330

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 31 e (new)

Motion for a resolution

Amendment

*31e. Repeats its call to create a
Directorate-General (DG) on defence and
space within the European Commission;
calls on the Commission to concentrate
the defence against Cyber attacks in this
future DG in order to protect EU data
links and own space capabilities, e.g.
Copernicus and Galileo;*

Or. en

Amendment 331

Antonio López-Istúriz White, Michael Gahler

Motion for a resolution

Paragraph 31 f (new)

Motion for a resolution

Amendment

*31f. Recalls the need to ensure that the
European Defence fund is kept on, or
even boosted in the next multi-annual
financial framework, with a sufficient
budget for Cyber defence;*

Or. en

Amendment 332
Antonio López-Istúriz White, Michael Gahler

Motion for a resolution
Paragraph 31 g (new)

Motion for a resolution

Amendment

31g. Calls for increased resources to modernize and streamline cyber security and intelligence dissemination between the European External Action Service/European Union Intelligence and Situation Centre (INTCEN), Council and Commission;

Or. en

Amendment 333
Anna Elżbieta Fotyga

Motion for a resolution
Subheading 6 b (new)

Motion for a resolution

Amendment

Public Private Partnership

Or. en

Amendment 334
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 31 h (new)

Motion for a resolution

Amendment

31h. Recognises that private companies play a key role in preventing, detecting, containing and responding to cyber security incidents, not just as an industry provider of technology but also including non-IT provision services;

Amendment 335
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 31 i (new)

Motion for a resolution

Amendment

31i. Recognises the private sectors role in preventing, detecting, containing and responding to cyber security incidents along with its role in stimulating innovation in cyber defence and thus calls for enhanced cooperation with the private sector to ensure shared insights of EU and NATO requirements and assistance in helping to find common solutions;

Or. en

Amendment 336
Anna Elżbieta Fotyga

Motion for a resolution
Paragraph 31 j (new)

Motion for a resolution

Amendment

31j. Calls on the EU to perform a comprehensive review of software, IT and communications equipment and infrastructure used in the institutions in order to exclude potentially dangerous programs and devices and to ban the ones that have been confirmed as malicious, such as Kaspersky Lab;

Or. en

Amendment 337
Jean-Luc Schaffhauser

Motion for a resolution
Paragraph 32

Motion for a resolution

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

Amendment

32. Instructs its President to forward this resolution ***confirming the responsibility of the Member States, to the Member States***, the European Council, the Council, the Commission, the VP/HR, the NATO Secretary-General ***in order to exclude this body from any cooperation in this field exclusive to the European Union***, the EU agencies in the fields of defence and cyber security, and national parliaments of EU Member States.

Or. fr

Amendment 338
Clare Moody, Wajid Khan

Motion for a resolution
Paragraph 32

Motion for a resolution

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

Amendment

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

Or. en