Amendment 11
Pedro Marques, Sven Mikser, Javi López
on behalf of the S&D Group

Report
Nathalie Loiseau
Implementation of the common security and defence policy – annual report 2021
(2021/2183(INI))

Motion for a resolution
Paragraph 43

43. **Condemns the malicious acts committed against Member States, such as hybrid attacks instrumentalising migration;** calls on the Union and the Member States to improve their capabilities to identify hybrid threats; insists that the Union and the Member States react firmly and in a coordinated manner against any new malicious, illegal or destabilising cyber-activity by making full use of the instruments available to the EU and in coordination with its partners; calls on Member States to improve national cyber defence capabilities; calls on the Union to work towards the creation of a legal instrument to respond to hybrid threats and to develop a comprehensive cyber-capacity including secure networks, communications and information-sharing, training and exercises, including through PESCO projects, and making good use of the EU cyber-diplomacy toolbox; calls for an urgent revision of the cyber defence policy framework in order to increase the prevention, attribution, deterrence and responsiveness capacity of the Union and its Member States by strengthening their position, situational awareness, tools and procedures; underlines the need for all EU institutions and EU Member States to cooperate at all levels to build a cybersecurity strategy, whose main objective should be to further strengthen resilience, and to develop common, and
resilience, and to develop common, and also better, national, robust civilian and military cyber-capabilities and cooperation in order to respond to lasting security challenges; welcomes therefore the 2021 SOTEU announcement of a European cyber defence policy; welcomes the increased cooperation among Member States on cyber defence in the framework of PESCO, including cyber rapid response teams; recalls that the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber-operational capabilities, as well as adequate responses to attacks against military installations, missions and operations; recognises that, to a certain degree, cyber defence is more effective if it also contains some offensive means and measures, provided that their use is compliant with international law; is concerned about the dependence of the EU and its Member States on foreign tools to guarantee their cybersecurity; stresses the need to foster a cybersecurity culture within European public and private entities, including through the introduction of devoted courses and curricula; notes the important training work carried out by the European Security and Defence College (ESDC) on cyber defence, and welcomes in this respect the establishment of the cyber education, training, evaluation and exercise (ETEE); stresses that ESDC should benefit from structural Union funding in order to be able to enhance its contribution to fostering the EU’s cyber defence skills, especially given the increased need for top level cyber experts; recognises the growing importance of cyber and automated intelligence capabilities; stresses that these are threats to all the Member States and EU institutions; urges all EU institutions and Member States to continue to improve their cyber and automated technologies, and further encourages cooperation on these technological advances; recommends that also better, national, robust civilian and military cyber-capabilities and cooperation in order to respond to lasting security challenges; welcomes therefore the 2021 SOTEU announcement of a European cyber defence policy; welcomes the increased cooperation among Member States on cyber defence in the framework of PESCO, including cyber rapid response teams; recalls that the successful implementation of EU missions and operations is increasingly dependent on uninterrupted access to a secure cyberspace, and thus requires robust and resilient cyber-operational capabilities, as well as adequate responses to attacks against military installations, missions and operations; recognises that, to a certain degree, cyber defence is more effective if it also contains some offensive means and measures, provided that their use is compliant with international law; is concerned about the dependence of the EU and its Member States on foreign tools to guarantee their cybersecurity; stresses the need to foster a cybersecurity culture within European public and private entities, including through the introduction of devoted courses and curricula; notes the important training work carried out by the European Security and Defence College (ESDC) on cyber defence, and welcomes in this respect the establishment of the cyber education, training, evaluation and exercise (ETEE); stresses that ESDC should benefit from structural Union funding in order to be able to enhance its contribution to fostering the EU’s cyber defence skills, especially given the increased need for top level cyber experts; recognises the growing importance of cyber and automated intelligence capabilities; stresses that these are threats to all the Member States and EU institutions; urges all EU institutions and Member States to continue to improve their cyber and automated technologies, and further encourages cooperation on these technological advances; recommends that
technological advances; recommends that options to foster the cyber capability-building of our partners should be explored, such as extending the mandate of EU training missions to also comprise cyber defence issues or launching civilian cyber missions; welcomes the imposition of sanctions against Russian, Chinese and North Korean perpetrators of cyber-attacks, including WannaCry, NotPetya and Operation Cloud Hopper;
9.2.2022 A9-0358/12

Amendment 12
Pedro Marques, Sven Mikser, Javi López
on behalf of the S&D Group

Report A9-0358/2021
Nathalie Loiseau
Implementation of the common security and defence policy – annual report 2021
(2021/2183(INI))

Motion for a resolution
Paragraph 62

Motion for a resolution  
62. Calls for EU Member States to aim to ensure that their national defence budgets amount to at least 2 % of their GDP;

Amendment
62. Calls for EU Member States that are NATO Allies to aim to ensure that their national defence budgets amount to at least 2 % of their GDP;

Or. en
Amendment 13
Pedro Marques, Sven Mikser, Javi López
on behalf of the S&D Group

Report
Nathalie Loiseau
Implementation of the common security and defence policy – annual report 2021
(2021/2183(INI))

Motion for a resolution
Paragraph 67

Motion for a resolution

Amendment

67. Backs the Commission proposal for VAT exemption for defence equipment designed and developed within the EU, which is a positive measure seeking to standardise practices at global level and foster European strategic autonomy;

deleted

Or. en
Amendment 14
Pedro Marques, Sven Mikser, Javi López
on behalf of the S&D Group

Report
Nathalie Loiseau
Implementation of the common security and defence policy – annual report 2021 (2021/2183(INI))

Motion for a resolution
Paragraph 96

Motion for a resolution

96. Will pay particular attention to ensuring that the special nature of military affairs is better reflected in European Union law; recalls, to this end, that Parliament is in favour of preserving the military’s status, which meets the very specific requirements of the military profession and constitutes the guarantee of the armed forces’ effectiveness in each of the Member States; calls for the intelligence services’ intervention capacities to be preserved, as these services cannot carry out their task of protecting national security without retaining access to connection data provided in full, as a preventive measure, for a sufficient period of time and under the supervision of the national courts and the European Convention on Human Rights; takes notes of Council’s adoption of its general approach on the Single European Sky package; recalls the need to safeguard Member States’ sovereignty and European armed forces’ freedom to act; recalls, in respect of the provision of services, the national security imperatives relating to access, reliability and integrity of data, and insists that the inclusion of military safeguard clauses in EU regulations should make it possible to meet this twofold challenge;

Amendment

96. Will pay particular attention to ensuring that the special nature of military affairs is better reflected in European Union law; recalls, to this end, that Parliament is in favour of preserving the military’s status, which meets the very specific requirements of the military profession and constitutes the guarantee of the armed forces’ effectiveness in each of the Member States; calls for the intelligence services’ intervention capacities to be preserved under the supervision of the national courts and the European Convention on Human Rights; takes notes of Council’s adoption of its general approach on the Single European Sky package; recalls the need to safeguard Member States’ sovereignty and European armed forces’ freedom to act; recalls, in respect of the provision of services, the national security imperatives relating to access, reliability and integrity of data, and insists that the inclusion of military safeguard clauses in EU regulations should make it possible to meet this twofold challenge;