OPINION

of the Committee on Foreign Affairs

for the Committee on Legal Affairs

with recommendations to the Commission on framework of ethical aspects of artificial intelligence, robotics and related technologies

(2020/2012(INL))

Rapporteur for opinion (*): Urmas Paet

(*) Associated committee – Rule 57 of the Rules of Procedure

(Initiative – Rule 47 of the Rules of Procedure)
SUGGESTIONS

The Committee on Foreign Affairs calls on the Committee on Legal Affairs, as the committee responsible:

– to incorporate the following suggestions into its motion for a resolution:

1. Highlights that the security and defence policies of the European Union and its Member States are guided by the principles enshrined in the European Charter of Fundamental Rights and those of the United Nations Charter, and by a common understanding of the universal values of respect for the inviolable and inalienable rights of the human person, human dignity, of freedom, of democracy, of equality and of the rule of law; highlights that all defence-related efforts within the Union framework must respect those universal values whilst promoting peace, security and progress in Europe and in the world; is of the opinion that the use of AI should be based on a common set of ethical principles according to which the use should be: responsible, equitable, traceable, reliable, and governable;

2. Welcomes the endorsement, by the 2019 Meeting of High Contracting Parties to the United Nations Convention on Certain Conventional Weapons (CCW), of 11 Guiding Principles for the development and use of autonomous weapons systems; regrets however the failure to agree on a legally binding instrument regulating lethal autonomous weapons (LAWS), with an effective enforcement mechanism; welcomes and supports the Commission’s High-Level Expert Group on Artificial Intelligence ‘Ethics Guidelines for Trustworthy AI’ published on 9 April 2019 and its position on lethal autonomous weapon systems (LAWS); urges Member States to develop national strategies for the definition and status of lethal autonomous weapons (LAWS) towards a comprehensive strategy at Union level and to promote, together with the Union’s High Representative/Vice-President of the Commission (‘HR/VP’), and the Council to the discussion on LAWS in the UN CCW framework and other relevant fora and the establishment of international norms regarding the ethical and legal parameters of the development and use of fully autonomous, semi-autonomous and remotely operated lethal weapons systems; recalls in this respect its resolution on autonomous weapons of 12 September 2018 and calls once again for the urgent development and adoption of a common position on lethal autonomous weapon systems, for an international ban on the development, production and use of lethal autonomous weapon systems enabling strikes to be carried out without meaningful human control and without respect for the human-in-the-loop principle, in line with the statement of the world’s most prominent AI researchers in their open letter from 2015; welcomes the agreement of Council and Parliament to exclude lethal autonomous weapons ‘without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes’ from actions funded under the European Defence Fund; believes that ethical aspects of other AI-applications in defence, such as intelligence, surveillance and reconnaissance (ISR) or cyber operations must not be overlooked, and special attention must be paid to the development and deployment of drones in military operations;

3. Recommends that any European framework regulating the use of artificial intelligence...
(AI)-enabled systems in defence, both in combat and non-combat situations, must respect all applicable legal regimes, in particular international humanitarian law and international human rights law, and it must be in compliance with Union law, principles and values; stresses that the Union should play a global role in leading the way towards a credible and binding AI regulatory framework rooted in democratic values and a human-centric approach; calls on the Union and its Member States to develop joint mechanisms to quickly and thoroughly assess the inherent AI-related risks and opportunities with regard to the application of Union law, inspired by the best practices of more advanced Member states, and to provide for necessary adjustment and enforcement where needed, keeping in mind the disparities in terms of technical and security infrastructures throughout the Union;

4. Recognises that unlike defence industrial bases, critical AI innovations could come from small Member States, thus a CSDP-standardized approach should ensure that smaller Member States and SME’s are not crowded out. Stresses that a set of common EU AI capabilities matched to a Member States operating concepts can bridge the technical gaps that could leave out states lacking the relevant technology, industry expertise or the ability to implement AI systems in their defence ministries;

5. Emphasises that the geographical scope of such a framework should cover all the components of artificial intelligence, robotics and related technologies developed, deployed or used in the Union, including in cases where part of the technologies might be located outside the Union or not have a specific location;

6. Underlines that emerging technologies not covered by international law should be judged by the principle of respect for humanity and the dictates of public conscience; underlines that the use and the ethics of AI-enabled systems in defence must be constantly assessed, from the point of view of human rights notably human safety, health and security, freedom, privacy, integrity and dignity and constantly monitored, especially from the point of view of its advantages and disadvantages, as well as its impact on the protection of universal human rights; believes that technological advantages in the field of AI-enabled systems in defence must go hand in hand with an ample discussion on the use of AI and its impact on societies and communities and potential economic and societal benefits, and the risks stemming from the use of AI must be properly communicated;

7. Considers that current and future security and defence-related activities within the Union framework will draw on AI, on robotics and autonomy, and on related technologies and that reliable, robust and trustworthy AI could contribute to a modern and effective military; the Union must therefore assume a leading role in research and development of AI systems in the security and defence field; believes that the use of AI-enabled applications in security and defence could offer a number of direct benefits to the operation commander, such as higher quality collected data, greater situational awareness, increased speed for decision-making, reduced risk of collateral damage thanks to better cabling, protection of forces on the ground, as well as greater reliability of military equipment and hence reduced risk for humans and human casualties; stresses that the development of reliable AI in the field of defence is essential for ensuring European strategic autonomy in capability and operational areas; recalls that AI systems are also becoming key elements in countering emerging security threats, such as cyber
and hybrid warfare both in the online and offline spheres; underlines at the same time all the risks and challenges of unregulated use of AI; notes that AI could be exposed to manipulation, to errors and inaccuracies;

8. Calls for synergies and networks to be established between the various European research centres on AI as well as other multilateral fora, such as the Council of Europe, the United Nations Educational Scientific and Cultural Organization (UNESCO), the Organisation for Economic Co-operation and Development’s (OECD), the World Trade Organisation and the International Telecommunications Union (ITU), in order to align their efforts and to better coordinate the development of the AI technology;

9. Stresses that AI technologies are, in essence, dual use, and the development of AI in defence-related activities benefits from exchanges between military and civil technologies; highlights that AI in defence-related activities is a transverse disruptive technology the development of which may provide opportunities for the competitiveness and the strategic autonomy of the Union;

10. Highlights that, based on the Commission’s communication of 8 April 2019 ‘Building Trust in Human-Centric AI’, whereby technology fully respects human rights and humans retain authority over automated decision-making systems, while complementing and supporting human autonomy and decision making the Union needs a robust AI regulatory framework focused on security and defence, following a path of responsibility and transparency, of protecting our citizens and their data, and of defending our values, that its policies aim at preserving peace, preventing conflicts and strengthening international security, whilst seizing the opportunities that those technologies offer, as well as realising that AI-enabled systems will be a key element in future defence-developments and defensive capabilities;

11. Calls on the Member States and the Commission to ensure that the algorithms used in defence systems, while keeping the necessary confidentiality, are governed by the principle of transparency, including a clear liability regime for the results of AI use; underlines that such algorithms must be constantly adjusted to the progress in AI technologies;

12. Underlines that the Union must be at the forefront of supporting multilateral efforts in the framework of the UN CCW Governmental Expert Group and other relevant fora, to discuss an effective international regulatory framework that ensures meaningful human control over autonomous weapon systems in order to master those technologies by establishing well defined, benchmark-based processes and adopting legislation for their ethical use, in consultation with military, industry, law enforcement, academia and civil society stakeholders, to understand the related ethical aspects and to contain the inherent risks of such technologies and prevent use for malicious purposes; those include in particular unintended harm to persons, be it material or immaterial, such as breach of fundamental rights or physical harm; the Union working together with the Member States must determine the appropriate liability regimes applicable to innovations in AI and other immersive technologies in the field of security and defence, thus establishing a legal basis for accountability and traceability mechanisms; highlights that Union legislation and normative frameworks must not be overtaken by any future technological advances, progress in AI and new methods of warfare and hence must be
supported by meaningful monitoring schemes to be constantly adjusted to prevent legal loopholes or grey zones; underlines that further AI research and development should ensure that AI enabled systems are better equipped to understand unique contexts;

13. Endorses the key principle “ethics-by-design”, by which ethical principles are embedded into AI products and services from the outset of the design process;

14. Recalls that most of the current military powers worldwide have already engaged in significant R&D efforts related to the military dimension of AI; considers that the Union must see to it that it does not lag behind in this regard; stresses that for any defence application of AI enabled systems, the Union should set technical and organisational standards, in accordance with the principle of “Security by Design”, allowing for specific human oversight, to ensure the resilience of such systems against vulnerabilities that can be exploited by external attacks, cyber-attacks and digital influence targeting the data, the model or the underlying infrastructure, both software and hardware, as well as their compliance with the highest possible reliability standards, active monitoring and supervision as regards the collection, storage and exploitation of operational data throughout a system’s entire lifecycle; emphasises the importance for transparency and accountability of AI algorithms; notes the important distinction between transparency of algorithms and transparency of the use of algorithms; stresses that AI systems and applications intended to extract and synthesise data, and extrapolate results therefrom to inform decisions for matters relating to defence and national security, must be specific in scope and comply with the provisions set out in the current regulatory framework in terms of gathering and processing data; stresses that AI applications designed to process data for intelligence purposes in defence related activities should comply with data processing standards to avoid risks of unintended surveillance or infringement of individual rights; believes that for high-risk applications of AI-enabled technologies like facial recognition which lack a definitive regulatory framework at the EU level, the Union must ensure that their development and deployment is rightful, proportional and respects the rights of individuals; stresses that competent national law enforcement authorities must respect relevant legislation while developing and deploying AI-enabled systems and technologies to maintain public order so as to mitigate the disproportionate risks of predictive policing; recognises that the primary guarantor of Euro-Atlantic security is NATO and calls for increased cooperation within the NATO Alliance for the establishment of common standards and interoperability of AI systems in defence; stresses that the transatlantic relationship is crucial in preserving shared values and in countering future and emerging threats;

15. Highlights the need to adopt clear reliability, safety and security provisions and requirements with proper certifications for AI-systems in security and defence, to introduce transparency criteria in the various phases, namely design, production and operation, and to carry out constant monitoring, regular tests and verification throughout the entire life cycle; underlines the necessity of ensuring compliance with applicable standards and obtained certifications where AI modifies e.g. through machine learning the functionality and behaviour of systems in which it is integrated, in order to ensure full traceability, explicability and accountability of decisions made with involvement of AI and their outcomes, as well as meaningful human control when such systems could kill humans;
16. Calls on the Commission to embed cybersecurity capacity-building in its industrial policy in order to ensure the development and deployment of safe, resilient and robust AI-enabled and robotic systems; calls on the Commission to explore the use of blockchain-based cybersecurity protocols and applications to improve the resilience, trust and robustness of AI infrastructures through disintermediated models of data encryption; encourages European stakeholders to research and engineer advanced features that would facilitate the detection of corrupt and malicious AI-enabled & robotics systems which could undermine the security of the Union and of citizens;

17. Stresses that all AI-systems in defence must have a concrete and well-defined mission framework, whereby humans retain the agency to detect and disengage or deactivate deployed systems should they move beyond the mission framework defined and assigned by a human commander, or engage in any escalatory or unintended action; considers that AI-enabled systems, products and technology intended for military use should be equipped with a ‘black box’ to record every data transaction carried out by the machine;

18. Underlines that the entire responsibility and accountability for the decision to design, develop, deploy and use AI-systems must rest on human operators, as there must be meaningful human monitoring and control over any weapon system and human intent in the decision to use force in the execution of any decision of AI-enabled weapons systems that might have lethal consequences; underlines that human control should remain effective for the command and control of AI-enabled systems, following the human-in-the loop, human-on-the loop and human-in-command principles at the military leadership level; stresses that AI-enabled systems must allow the military leadership of armies to assume its full responsibility and accountability for the use of lethal force and exercise the necessary level of judgment, which machines cannot be endowed with as it must be based on distinction, proportionality and precaution, for taking lethal or large-scale destructive action by means of such systems; stresses the need to establish clear and traceable authorisation and accountability frameworks for the deployment of smart weapons and other AI-enabled systems, using unique user characteristics like biometric specifications to enable deployment exclusively by authorised personnel;

19. Calls on the Commission to work together with Member States’ national competent authorities and other stakeholders participating in the development and deployment of AI-enabled systems, products and technologies to establish a safe, secure and resilient framework whereby the source code of AI-enabled systems is shared, monitored and verified to mitigate potential deviations from the governing principles and ethical framework underpinning AI technology in the field of security and defence; suggests to the Commission that the Union must retain ownership of the intellectual property of Union-funded research on AI-enabled systems, products and technologies in security and defence;

20. Underlines that the Union must promote better understanding of the military implications, advantages and opportunities and weaknesses of AI, of robotics and of autonomous functions and features, including the potential for the European defence industry, by working alongside military officials; considers that the Union needs to promote the acquisition of the necessary skills and knowledge on technology
development processes and operational methods throughout the supply chain and over the full lifecycle of AI-enabled military capabilities; underlines the urgent need for establishing increased European strategic and technological independence in the field of AI-enabled systems, including the critical infrastructure it relies on;

21. Believes that enhanced cooperation between Member States and the Commission is necessary to guarantee coherent cross-border rules in the Union, to encourage the collaboration between European industries and allow the development and deployment of AI-enabled technologies consistent with the prescribed safety and security standards, and the ethical framework governing the development and deployment of AI technology;

22. Recognises, in the hybrid and advanced warfare context of today, that the volume and velocity of information during the early phases of a crisis might be overwhelming for human analysts and that an AI system could process the information to ensure that human decision-makers are tracking the full spectrum of information within an appropriate timeframe for a speedy response;

23. Underlines the importance of investing in the development of human capital for artificial intelligence, fostering the necessary skills and education in the field of security and defence AI technologies with particular focus on ethics of semi-autonomous and autonomous operational systems based on human accountability in an AI-enabled world; stresses in particular the importance of ensuring that ethicists in this field have appropriate skills and receive proper training; calls on the Commission to present as soon as possible its "Reinforcement of the Skills Agenda", announced in the White Paper on Artificial Intelligence on the 19th February 2020;

24. Stresses that quantum computing could represent the most revolutionary change in conflict since the advent of atomic weaponry and thus urges that the further development of quantum computing technologies be a priority for the Union and Member States; recognises that acts of aggression, including attacks on critical infrastructure, aided by quantum computing will create a conflict environment in which the time to make decisions will be compressed dramatically from days and hours to minutes and seconds, forcing Member States to develop capabilities that protect themselves and train both its decision makers and military personnel to respond effectively within such timeframes;

25. Stresses the need to overcome the current fragmentation within the Union as regards national AI-related law, research, innovation and expertise in the area of AI, which endangers the functioning of the internal market and the objective of ensuring that there is reliable and secure development of AI in Europe; in this respect welcomes the inclusion of AI-related projects under the European Industrial Development Programme(EDIDP); believes that the future European Defence Fund (EDF) and the Permanent structured cooperation (PESCO) also offer well adapted frameworks for future AI-related projects that would help to better streamline Union efforts in this field, and promote at the same time the Union’s objective of strengthening human rights, international law, and multilateral solutions; stresses that AI-related projects should be synchronized with the wider Union civilian programmes devoted to AI; notes that in line with the European Commission’s White Paper on AI excellence and testing centres
concentrating on research and development of AI in the field of security and defence should be established with vigorous specifications underpinning the participation of and investment from private stakeholders;

26. Highlights that the Union needs to strive for strategic resilience so that it is never again found unprepared in times of crisis, and underlines that, especially in as far as artificial intelligence and its application to defence and security are concerned, this is of crucial significance; emphasises that supply-chains for AI systems in defence and security that can lead to technological dependence should be recalibrated and such dependencies should be phased-out; calls for increased investment in European AI for defence and in the critical infrastructure that sustains it;

27. Emphasises that the development of AI that respects fundamental rights and supports the public interest requires the strategic pooling and sharing of data in the Union between private and public entities, as well as the strengthening of a Union AI ecosystem, which involves public, private, and civil society stakeholders; calls on the Commission to foster dialogue, closer cooperation and synergies among Member States, researchers, academics, civil society actors and the private sector, in particular leading companies and enterprises, and the military so as to have inclusive policymaking processes when it comes to defence-related AI regulations, harness the potential of AI to the fullest, while fostering a better understanding of risks and benefits, as well as ensuring maximum operational security;

28. Highlights that, in the context of the widespread disinformation war, particularly driven by non-European actors, AI technologies might have ethically adverse effects by exploiting biases in data and algorithms or by deliberately alternating learning data by a third country, and could be also exposed to other forms of dangerous malign manipulation in unpredictable ways and with incalculable consequences; there is therefore an increased need for the Union to continue investment in research, analysis, innovation and cross-border and cross-sector knowledge transfer in order to develop AI technologies that would be clearly void of any sort of profiling, bias and discrimination, and could effectively contribute to combating fake news and disinformation, while at the same time respecting data privacy and the European legal framework;

29. Stresses the importance of the creation of an ethical code of conduct underpinning the deployment of weaponised AI-enabled systems in military operations, similar to the existing regulatory framework prohibiting the deployment of chemical and biological weapons; is of the opinion that the Commission should initiate the creation of standards on the use of AI-enabled weapons systems in warfare in accordance with international humanitarian law, and the Union should pursue the international adoption of such standards; considers that the Union should engage in AI diplomacy in international fora with like-minded partners like the G7, the G20, and the OECD;

30. Takes note of the Commission's White Paper on Artificial Intelligence of 19 February 2020 and regrets that military aspects were not taken into account; calls on the Commission and on the HR/VP to present, also as part of an overall approach, a sectoral AI strategy for defence-related activities within the Union framework, that ensures both respect for citizens’ rights and the Union’s strategic interests, and that is based on a consistent approach spanning from the inception of AI-enabled systems to their military
uses, and to establish a Working Group on Security and Defence within the High-Level Expert Group on Artificial Intelligence that should specifically deal with policy and investment questions as well as ethical aspects of AI in the field of security and defence; calls on the Council, the Commission and on the VP/HR to enter in a structured dialogue with Parliament to that end.
INFORMATION ON ADOPTION IN COMMITTEE ASKED FOR OPINION

<table>
<thead>
<tr>
<th>Date adopted</th>
<th>22.6.2020</th>
</tr>
</thead>
</table>
| Result of final vote | +: 60  
|                    | -: 7   
|                    | 0: 2    |
| Substitutes present for the final vote | Katarina Barley, Nicolas Bay, Arnaud Danjean, Katrin Langensiepen, Hannah Neumann, Mick Wallace |
### FINAL VOTE BY ROLL CALL IN COMMITTEE ASKED FOR OPINION

<table>
<thead>
<tr>
<th>60</th>
<th>+</th>
</tr>
</thead>
<tbody>
<tr>
<td>S&amp;D</td>
<td>Maria Arena, Katarina Barley, Włodzimierz Cimoszewicz, Tanja Fajon, Raphaël Glucksmann, Dietmar Köster, Claudiu Manda, Sven Mikser, Tonino Picula, Kati Piri, Giuliano Pisapia, Nacho Sánchez Amor, Isabel Santos, Andreas Schieder, Sergei Stanishev</td>
</tr>
<tr>
<td>RENEW</td>
<td>Petras Aušrevičius, Katalin Cseh, Klemen Groselj, Bernard Guetta, Ilhan Kyuchyuk, Nathalie Loiseau, Javier Nart, Urmas Paet, María Soraya Rodríguez Ramos, Hilde Vautmans</td>
</tr>
<tr>
<td>ID</td>
<td>Anna Bonfrisco, Susanna Ceccardi</td>
</tr>
<tr>
<td>VERTS</td>
<td>Alviina Alametsä, Reinhard Bütikofer, Katrin Langensiepen, Hannah Neumann, Diana Riba i Giner, Tineke Strik, Thomas Waizt</td>
</tr>
<tr>
<td>ECR</td>
<td>Anna Fotyga, Karol Karski, Jacek Saryusz-Wolski, Hermann Tertsch, Witold Jan Waszczykowski, Charlie Weimers</td>
</tr>
<tr>
<td>NI</td>
<td>Fabio Massimo Castaldo, Márton Gyöngyösi</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>7</th>
<th>-</th>
</tr>
</thead>
<tbody>
<tr>
<td>GUE</td>
<td>Stelios Kouloglou, Manu Pineda, Idoia Villanueva Ruiz, Mick Wallace</td>
</tr>
<tr>
<td>ID</td>
<td>Nicolas Bay, Thierry Mariani</td>
</tr>
<tr>
<td>NI</td>
<td>Kostas Papadakis</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>2</th>
<th>0</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID</td>
<td>Lars Patrick Berg, Harald Vilimsky</td>
</tr>
</tbody>
</table>

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