SPECIAL COMMITTEE ON ARTIFICIAL INTELLIGENCE IN A DIGITAL AGE (AIDA)

Joint hearing on the external policy dimension of AI

PANEL II
with the SEDE Sub-Committee

AI, CYBERSECURITY AND DEFENCE

***

Mircea Geoană, Deputy Secretary General, NATO

François Arbault, Director for Defence Industry, DG DEFIS, European Commission

Pieter Elands, Program Manager Unmanned Systems, TNO (Dutch Research Institute)

Elizabeth Minor, Advisor, Article 36 NGO

Gilman Louie, Commissioner, U.S. National Security Commission on Artificial Intelligence (NSCAI)

Anja Dahlmann, Head of Project - International Panel on the Regulation of Autonomous Weapons (IPRAW), German Institute for International and Security Affairs

BRUSSELS

THURSDAY 4 MARCH 2021

1-002-0000

IN THE CHAIR: DRAGOŞ TUDORACHE

Chair of the Special Committee on Artificial Intelligence in a Digital Age

(The meeting opened at 13.47)

1-003-0000

Chair. – Good afternoon again to all Members. Today we are joined by members of AIDA, of course, our Committee on Artificial Intelligence in the Digital Age, as well as members of the Subcommittee on Security and Defence (SEDE). I would like to warmly welcome everyone who is following this event from both committees and look forward to, certainly, a lively debate.

On that note, I would also like to extend a warm welcome to our panellists. We have a distinguished panel with us today. We have high-level institutional representation from NATO, from the European Commission, and the US National Security Commission on AI. This institutional perspective will be invaluable to all Members who are grappling with the complex questions raised by AI in this domain. We will also hear from scientific experts as well as civil society. These are important contributions to the topic of today's discussion.

The previous seminar, with the Committee on Foreign Affairs (AFET) on the external and diplomacy dimension of AI, and the present one are logically connected because they are both about the way our digital goals have evolved to the point where they become key considerations of our foreign security and defence policies. And it is also about the transatlantic relationship and how Europe and the US can work together to set the playing field in new technologies, and about the topics we can, and should, engage with in international fora such as the OECD, the G7, the G20, the UN and standard-setting institutions, and with like-minded partners such as the UK, Canada, Australia, New Zealand, Japan, South Korea and others.

In an increasingly interconnected world, cybersecurity is key to our strategic resilience in our overall security. We cannot reap the full benefits of the digital transformation if we are dependent in Europe on foreign technology from states who do not share our values and if we have vulnerabilities in our critical infrastructure and digital infrastructure. Beyond securing our digital infrastructure, we need to be mindful to the fact that AI can be, and is being, used for increasingly sophisticated cyberattacks. We need to develop capabilities at the European level as well as at the US level, I am sure, but also in partnership with our allies to be able to counter such attacks and to deter others, both states and non-state actors, from launching such attacks against us.

This is still a grey area in international conflict, but we need to work to strengthen our joint response to such attacks. European action, however, needs to be taken, keeping a key element in mind – interoperability with NATO and our strategic allies – and is doing more than any other. Setting the standards and defining the rulebook is key to our long-term resilience and security. And these standards need to be in accordance with our shared values, values on which our societies are founded: individual freedom, fundamental rights, democracy and the rule of law. This will also inform our decision on what we can and cannot use AI for. For example, lethal autonomous weapons systems is a path we should ensure no one pursues at the global level.

I will now pass the floor to my colleague, the SEDE Chair, Ms Nathalie Loiseau. Natalie, you have the floor. Please try and stick to five minutes.

1-004-0000

Nathalie Loiseau (Renew), *Chair of the Subcommittee on Security and Defence (SEDE).* — Mr President, dear Dragoş, dear colleagues, first of all, I would like to say how happy I am to

be attending this joint meeting with the AIDA Special Committee and the Subcommittee on Security and Defence (SEDE) on such an important topic and one which SEDE has been following very closely for some time.

Of course, not a day goes by without talk of artificial intelligence and what it promises to revolutionise in our lives. We also know that artificial intelligence, or enhanced intelligence as I would call it, is the subject of a strategic competition. It is in the process of becoming an instrument of technological, economic and also military power.

To ensure its strategic autonomy, Europe therefore has an incentive to invest rapidly and on a massive and coordinated scale in the use of artificial intelligence. However, we must bear in mind that its use by other powers, but also by non-state actors, for unfriendly or hostile – and in any case undemocratic – purposes has become a reality.

The European Union must therefore define its own use of artificial intelligence – artificial intelligence that respects our values, principles and international law – in a context that has become particularly dynamic. This is particularly true in the field of defence. In this sector, there may be opportunities for the use of artificial intelligence. Artificial intelligence systems can improve the decision-making process through faster and more reliable data collection and interpretation. They can reduce the response time for combat operations and improve respect for the law of armed conflict by improving the targeting of legitimate military objectives and thereby further protecting the civilian population and military personnel.

Artificial intelligence is also of great use in real-time analysis of cyber threats, data and image processing or electronic warfare operations. Through Horizon Europe and the European Defence Fund, we can join the forces of our research laboratories and our defence industries to develop cutting-edge European artificial intelligence. On 22 February, the Commission launched its first ever action plan on synergies between the civil, space and defence industries. This plan is intended to strengthen Europe's technological leadership by exploring and exploiting the disruptive potential of technologies such as cloud, processors, cyber intelligence, quantum intelligence and artificial intelligence.

In this constant search for more and more automation, we simply need to ask ourselves a question: can we let artificial intelligence applications act autonomously? What degree of autonomy can we allow? The use of autonomous AI-enabled systems may also have unexpected consequences by manipulating learning data or even as a result of cognitive biases transmitted by humans to algorithms. This raises the key question of human control and accountability in, for example, the whole debate on lethal autonomous weapon systems.

On this topic, the European Parliament's position on ethical risks related to artificial intelligence is very clear. SEDE adopted two opinions in 2020 on the ethical aspects of artificial intelligence in the field of defence, which state that the development and use of lethal autonomous weapons without significant human control is not an option for the EU. The European Parliament wants discussions to continue under the Convention on the Prohibition or Restriction of the Use of Certain Conventional Weapons – the only way to achieve a universal, credible and effective framework for autonomous military systems, as we cannot rule out the risk that such weapons may be developed and used by irresponsible states and fall into the hands of non-state actors.

To conclude, I would say that artificial intelligence is a revolution in which the European Union must be firmly committed, at the risk of becoming dependent on other technologies controlled by sometimes hostile powers. But in order to do so we must strike a balance between ethics, accountability and infertility so that this technological development never taints trust in democracy.

1-005-0000
Chair. – We will now move on to the panel. A few housekeeping rules before we start. We have six Members on the panel. Each of them will have five minutes for their introductory remarks, then I will kindly ask them to stay with us for the rest of the hearing. We've organised the intervention of the Members for each of the political groups into slots. Each political group will have two slots, alternating AIDA members and SEDE members. Each Member will have a two minute-slot in which to put their question, and I also kindly ask them to direct their questions to ideally to one or maximum two of the panellists, so that they will then have the possibility to respond in one or two minutes, depending on whether there one question or two.

So, without further ado, I will introduce the panel. As I said, we have a number of distinguished guests on our panel today. There is the Deputy Secretary-General of NATO, Mr Mircea Geoană a very warm welcome to him; Mr François Arbault, Director for Defence Industry, DG DEFIS, European Commission; Pieter Elands, Programme Manager Unmanned Systems, TNO, Netherland's Organisation for Applied Scientific Research; Ms Elizabeth Minor, Advisor with Article 36 NGO; Gilman Louie, Commissioner with the US National Security Commission on Artificial Intelligence; and Anja Dahlmann, Head of Project International Panel on the Regulation of Autonomous Weapons, German Institute for International and Security Affairs.

With that, I give the floor to the first panellist, Deputy Secretary-General Mr Geoană. The floor is yours for five minutes.

1-006-0000
Mircea Geoană, *Deputy Secretary General, NATO***.** – I wish to thank the chairs and all the members of the two committees for inviting us, and myself, here today. I'm delighted to join this great panel from both sides of the Atlantic and to discuss an issue of such importance to our common security.

New technologies, including artificial intelligence, big data and autonomy are changing the way we live and work. They also change not only the way wars are waged and won, but the very definition of security. Today's developments differ from any previous defence innovation periods in that they are often dual use and largely driven by the civilian private sector, which was not the case in the past.

So technology and the world are moving fast and we must move even faster to maintain our edge. We must identify, understand and adopt new technologies at speed and scale, while mitigating any risks and any advantage potential adversaries and competitors might seek. This is exactly what we do here at NATO. At their last meeting in December 2019, NATO leaders adopted a comprehensive roadmap on emerging and disruptive technologies and at last month's Defence Ministerial meeting allies agreed a coherent strategy for its implementation.

It sets out ways to work with partners, academia and, of course, the private sector, to develop new technologies more quickly, strengthen our industrial base and protect against adversarial technology transfers. As part of his NATO 2030 initiative to future-proof our alliance, the Secretary General of NATO has proposed a NATO defence innovation initiative to promote better transatlantic cooperation on critical technologies. It is the only place that brings Europe and North America together every day. NATO is an important transatlantic forum for collaboration and coordination, also on emerging technologies, including on standards-setting.

To support our efforts, I have the pleasure of chairing NATO's Innovation Board, which brings together senior leaders from across the NATO enterprise. Our Secretary General has appointed an external extraordinary group of advisers to provide outside expertise and input to the challenges we all face.

Of the new technologies we are looking at, indeed AI is the most pervasive, especially when combined with other technologies like big data, autonomy or biotechnologies or human enhancement. So AI is the priority for our alliance. Russia and China are pursuing the development and adoption of AI at pace, with little regard for human rights and data privacy. We are seeing, with deep concern, the hostile use of new technologies.

NATO calls out such abuses when we see them – for example, last summer when the whole alliance condemned publicly destabilising and malicious cyber activities directed against those who, including hospitals, were working to respond to the COVID pandemic. So we need to find ways to maximise the undisputed opportunities AI offers while minimising the risks. This also means protecting our technological developments from adversarial, licit and illicit technology transfers. Our adversaries do not hesitate to use these technologies to undermine our security.

AI will revolutionise the way we defend ourselves, including by enhancing our intelligence analysis and situational awareness. Not only will it increase the amount and accuracy, it will also free up extra time to interpret rather than identify relevant data. This will depend on our willingness to share data. International organisations can play a key role in providing the necessary infrastructure to make data sharing more effective and, yes, more secure.

The effective use of AI will also require full trust between allies and also from our public opinions. So we need a common framework for the responsible use of AI, based on our democratic values and the rule of law. With these elements, we put ourselves in a position of strength, as democracies and open societies provide the best framework to enable and foster innovation. We have to put to work the power of regulations, and the US, in its freshly-announced Interim National Security Strategic Guidance, coins perfectly the issue at hand in saying: ‘Emerging technologies remain largely ungoverned by laws or norms designed to center rights and democratic values, foster cooperation, establish guardrails against misuse or malign action, and reduce uncertainty and manage the risk that competition will lead to conflict.’

We also welcome the recent proposal launched by the European Union for a new transatlantic agenda for global cooperation with the US, including on new technologies. Nevertheless, the regulatory powers of North America and Europe in the case of NATO – the gold standard for security and defence – and the huge power of USA regulatory power are such that we have to make sure we foster this innovation together, in concert, because only together will we be able to defend, shape and enforce a multinational system of world governance in the field of new technologies. So this challenge needs to be tackled in close collaboration between NATO and the EU, as well as individual Member States and allies.

Fostering and protecting AI developments calls upon the two organisations to strengthen our cooperation and remind us all that we, NATO and the EU, already enjoy a strategic partnership. I welcome the fact that both NATO and the EU have stepped up their efforts on the military use of AI in recent months. We also have witnessed increased engagement between NATO and EU, with our Secretary General attending, for the first time, the meeting of the College of Commissioners and Commissioner Vestager visiting NATO headquarters recently.

Next week, I will be co-chairing the NAC-PAC meeting on exactly the topic of new technologies. To maintain this engagement, I very much welcome the engagement with you today. Beyond that, I would also encourage you and your committees and your Members to cooperate also with the Parliamentary Assembly of NATO that has a specialised technology committee, which is a high-end, high class representation from national parliaments of the alliance.

This is a way in which we can identify best practices, identify potential synergies, including on developing appropriate regulatory framework, and setting transatlantic as well as global standards for the ethical use of AI.

By bringing together our innovation ecosystems, composed of incredible universities, vibrant start-ups and small and medium-sized enterprises on both sides of the Atlantic, we can foster an environment that ensures Europe and North America maintain our technological edge. We can ensure that security and prosperity for the almost one billion people that NATO is supposed to defend now and for the future.

Again, thank you so much for inviting me. I am very much personally committed to engaging with the European Parliament, with the EU institutions, with Member States, in order to keep this strategic partnership between EU and NATO vibrant and useful for both organisations.

1-007-0000

Pieter Elands, *Program Manager Unmanned Systems, TNO (Dutch Research Institute)***.** – I'm Pieter Elands, working for TNO in the Netherlands. I work on autonomous systems where the intelligence is made possible through AI. Next slide, please.

The term 'autonomous systems' may also be replaced by 'intelligent systems'. An important principle to remember when addressing autonomy is the principle of orthogonality, as presented by Nick Bostrom, the author of the famous book Superintelligence. It means a clear distinction between the 'what' and the 'how'. The 'what' means that humans decide what goals should be achieved in an operation or during a mission. The 'how' means that the machine is allowed to think of the best possible way to achieve these goals. In doing this, the machine is bound in its solution space by restrictions set by humans. This is the main principle to achieve meaningful human control and, while often overlooked, it's very important. All important academics in the field of autonomous systems support this principle. Next slide, please.

Using this principle, it is easy to debunk some popular frames. I will discuss two of these frames. The frame used most often concerns machines that decide to kill. If man decides the 'what' and specifies the boundaries for the machine, the machine must obey these restrictions. It's the human who may allow the machine to use violence within the boundaries set by man. And if killing one person prevents the death of hundreds of people, it could be allowable. But if a machine starts killing at random, it's a very poor design without meaningful human control. And a framework we invented, our framework for meaningful human control, discusses how to set goals to be achieved in combination with ethical and legal restrictions. We think it's possible to bound machines. Next slide, please.

A second misunderstanding is the frame that machines, which have self-learning algorithms, become unpredictable and hence uncontrollable. Again, this principle of orthogonality means that the human sets the restrictions a machine must obey. It may be able, through self-learning, to improve its ability to find good solutions, but it remains bound by the goal function set by man. To be sure, we recommend that self-learning is allowed only after the operation and not during the operation. But these frames are meant to get us worried. And I think the main worry is not about these frames, but how to achieve this meaningful human control. Next slide, please.

And this is the framework we designed at TNO. In this framework, there's not one human and not one loop. Several humans exercise a specific part of human control. The legislator sets the laws, such as the law of armed conflict and international humanitarian law, for instance prescribing proportionality and subsidiarity. In addition, the legislative power sets the ethical guidelines to be used in armed conflict. A combination of various ethical principles may be involved consequential ethics, normative ethics, virtue ethics, for example and this leads to what we call an ethical goal function, which includes all relevant legal aspects.

In addition, the legislator sets the military goals and the rules of engagement as a requirement for the military commander. The military commander combines these requirements with the ethical goal function into a so-called mission goal function. This mission goal function is then given to the machine or the human-machine team as their mission orders. It contains military goals and ethical and legal constraints. The machine or human-machine team will then execute the mission governed by the mission goal function. The machine or the human-machine team is unable to change this mission goal function. So, control and accountability is exercised before the mission through the green arrows, during the mission through the blue arrows and after the mission through the red arrows, in the form of explanations. And in case a fully autonomous system is being used, the blue arrows disappear. This is our idea, our example of how to exercise meaningful human control. Thank you.

1-008-0000

Elizabeth Minor, *Advisor, Article 36 NGO***.** – Thanks for having me. I'm speaking from Article 36, which is a UK-based NGO working for stronger standards of weapons and civilian protection, and we're part of the global campaign to stop killer robots. We were very pleased to see strong support from the European Parliament for an international treaty on autonomous weapons in its 2018 and 2021 resolutions, as well as support from the EU High-Level Expert Group on AI for a treaty. We think this sends an important signal to the EU and to European states.

In my five minutes I want to make three points about moving towards the international regulation of autonomous weapons systems, which include some military applications of AI, but also other systems. Firstly, the international discussion at the CCW, as mentioned, is now at a point where states must consider in detail how regulation could be structured. Secondly, effective international legal regulation in this area must include both positive obligations to maintain meaningful human control, and prohibitions on certain types of weapons systems. And thirdly, the European Defence Fund Regulation requirements on autonomous weapons systems should be boldly and progressively interpreted in putting these into practice, and I'll talk about that a bit more.

So firstly, though international discussion on autonomous weapons can be quite wide-ranging, in general, increasing autonomy brings challenges to human dignity, civilian protection and the law, the understanding of systems and responsibility in the use of force, and also to global peace and security. These are all global values and concerns that are important to Europe. There's now significant common ground among states acknowledging that collective work is needed to describe what human control over weapons systems is required to uphold legal principles and respond to ethical concerns. There is not, however, agreement on the need for an international legal instrument for regulation. Many states developing these capabilities have spoken against doing this, perhaps because they would prefer to have these systems before considering controls, despite the global risks we think this would carry.

We think that agreeing a treaty, even without all countries participating, would nevertheless be valuable. There's a real need at the moment to work through these complex issues and set clear and strong standards that can influence practice as well as future agreements. What's needed now is for countries to discuss in detail the content, substance and structure of an international treaty of regulation to draw these lines. Europe should seek to play a progressive role in this. The EU and European states position themselves as strong supporters of multilateralism and global rules, and Europe is already seeking to lead in standard-setting around emerging technologies.

Because autonomous weapons is an issue of systems and of configurations, rather than a clear class of physical weapons technologies, international regulation, we think, needs to include

both positive obligations on states to ensure control over weapons systems in a meaningful way and prohibitions on clearly unacceptable developments. Systems that cannot be controlled should, of course, be prohibited, and in our opinion so should autonomous systems that target people, as these would undermine human dignity and also threaten civilian protection.

In this context, it's significant to see the draft regulation establishing the European Defence Fund draw a legal line against supporting action for the development of certain autonomous weapons. This part of the regulation will need to be operationalised and put into practice.

Given that the regulation's definition could be read quite narrowly as addressing only systems without the possibility for meaningful human control and that are used in strikes against humans in particular, it would be beneficial to consider how it could be interpreted perhaps closer to the European Parliament's definition from 2018 to also address uncontrollable systems used for strike targets other than people, and also the much wider range of systems designed with the possibility for adequate control, but which could be deployed problematically in practice in the absence of clear rules. In any case, there is an opportunity to contribute to standard-setting on what constitutes a system that cannot be meaningfully controlled by humans, which is part of the problem at hand, and also to elaborate what meaningful human control over weapon systems should entail.

A process that is open to external advice and input on public proposals would be very important for putting this part of the EDF regulation into practice, and it should also be taken back to national capitals. European states and institutions should take the opportunity to lead progressively and to feed useful work at European level on this into international deliberations.

With the threat to global peace and security that autonomous weapons systems and the arms race to develop them poses, stronger international standards are essential. It's in the interests of progressive states to join together to create these standards and address the collective risks, and we think Europe should play a leading role in this process.

1-009-0000

Chair. – I would like to welcome Mr Gilman Louie. Good morning, sir. Thank you for agreeing to start the day with us. As Commissioner for the US National Security Commission on Artificial Intelligence, you'll understand that we very much look forward to hearing what you have to say. So if you are with us, you have the floor for five minutes.

1-010-0000

Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI).* – I want to thank you for the opportunity to appear here today as a member of the National Security Commission on Artificial Intelligence. The NSCAI was created by the US Congress to recommend methods to advance the development of AI, machine learning and associative technologies to comprehensively address the USA's national security and defence needs. The NSCAI submitted its final report to Congress and the President earlier this week. Our report presents an integrated strategy to reorganise the US Government, reorient the nation and rally our closest allies and partners to defend and compete in the coming era of AI-accelerated competition and conflict.

My message here today is straightforward. The United States, the EU and EU Member States must get AI right to further our shared democratic values, advance our economic prosperity and ensure national and international security. I begin with the observations about the very real threats that proliferation of AI-enabled capabilities carry for the free and open societies. AI will dramatically increase the speed and severity of cyber-attacks by giving hostile actors the power to coordinate multilayer attacks against our digital systems, at machine speed with adaptive agility. As our nations become more connected, our adversaries can execute cyber campaigns

powered by AI that could cripple our critical infrastructure, hijack our virtual and physical systems, steal sensitive data about our citizens, rob our IP and disable national defences.

Unlike 20th century propaganda, where one powerful message was sent to a million people, AI-enabled malign information campaigns will send 100 million individualised messages from tens of millions of fake social media accounts. These messages will be configured based on detailed profiles of the targets' physical and digital lives, emotional states, social networks and political affiliations. Sophisticated AI malign information campaigns will be used to increase the level of distrust in our institutions, blur the lines between fact and opinions, reinforce the echoes of hatred, interfere with democracy and destroy our social cohesion. Rival states are already trying out some of these techniques.

The reach of tools that certain states use to monitor, control and coerce their own citizens – big data analytics, surveillance and propaganda – can be extended beyond their borders and directed at foreigners. Without adequate data protections, AI makes it harder for anyone to hide their financial situations, pattern of daily life, relationships, health and even emotions. Personal and commercial vulnerabilities become national security weaknesses as adversaries map individuals' networks and social fissures and model how best to manipulate behaviour or cause harm.

At the same time, AI technologies are the most powerful tools in generations for expanding knowledge, increasing prosperity and enriching the human experience. The US and the EU must be partners in the global competition to defend digital democracies against digital authoritarianism and promote innovation grounded in our shared values. While there are challenges to the transatlantic relationship, there is much more that brings us together. A strong Europe is necessary for our collective security and prosperity. A high-level strategic dialogue and emerging technologies will foster consensus on ethics and create robust frameworks for joint research between American and European scientists. The dialogue can be a vehicle for the US and EU to bridge the gaps between our governments on core issues such as privacy and China. More broadly, the NSCAI has also proposed an emerging technology coalition of democratic nations. This coalition, working closely with the private sector and civil society, would provide a forum to shape international norms, align technical standards, coordinate innovation policies to advance openness, security, reliability, trustworthiness and democratic values. It would also provide a mechanism to further data-sharing and cross-border R&D and coordinate global investments in democratic digital infrastructure.

In addition, we need international coordination to address the discrete threats I mentioned earlier. The challenges to malign information operations and AI-enabled cyber threats require a global task force to share threat information, coordinate real-time responses and develop AI-enabled tools to certify content, authenticity and provenance. Through our defence of alliances such as NATO, the US and its allies must prioritise interoperability to avoid the risk that differential adoption of AI would undermine our collective defence and security.

Allies and must also work towards international standards for AI-enabled and autonomous weapons systems: standards that strive to reduce associated risks by ensuring responsible, safe and ethical developments and use that complies with international humanitarian law. We must ensure that only human beings can authorise the employment of nuclear weapons and the NSCAI supports constructive dialogue with competitors to advance strategic stability and reach agreement on this critical issue.

Decreased cooperation between the US and EU will only benefit strategic competitors. Greater cooperation on AI and emerging technologies will reinforce democratic values, encourage innovation, promote mutual economic growth and encourage strategic competitors like China

and Russia to conform to international norms and advance global security. Thank you, and I look forward to answering any questions.

1-011-0000

François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – Thank you very much, and I hope that you can hear me correctly; apologies for those technical issues. Thank you to the European Parliament for its invitation and shared interest in artificial intelligence, a topic that is, as you know, very much a priority also for the Commission and for Commissioner Breton.

The discussion on the balance between the need to tap the promising potential of artificial intelligence and the need for increased investment in Europe has to be balanced with the need to secure the trustworthy use of AI, and this balance is very important for the Commission. It takes, of course, a particular resonance for the EU defence industry and, as you know, one of the key tasks of DG DEFIS is to contribute to the strengthening of the European defence, technological and industrial base, and in particular to really support innovation. This is what we are doing through the implementation of the European Defence Fund (EDF), notably by fostering cooperation between the Member States in the field of defence, R&D and research and development.

So let me focus on how the use of AI is addressed in this specific framework and to elaborate a bit on the possibilities for funding in relation to research and development in projects involving AI under the EDF. The EDF has a budget of EUR 8 billion during the current MFF and it aims to support – and I insist on that very much – competitiveness and innovation. The stress on innovation means, of course, that we can expect the funding via the EDF of R&D actions related to emerging technologies and AI in particular.

AI is of course a key enabling technology for all defence capability areas. There is a very clear trend of digitisation of military operations and missions, and Europe's armed forces cannot afford to lag behind with these developments. Therefore, AI will very naturally be addressed in the EDF's annual work programmes across all defence capability domains. AI applications in defence – and this is very important to stress – are not only about killer robots or autonomous weapons systems. AI, on the contrary, can bring many benefits for the armed forces. It can enable faster and better information and decision-making by ensuring collaborative warfare. It can also provide for greater protection of soldiers from risky tasks or provide for systems that can take care of routine and very often dangerous tasks.

The two windows in the EDF the Preparatory Action on Defence Research and the European Defence Industrial Development Programme (EDIDP) have already provided funding for AI-related defence projects. So we are not starting from scratch and an AA-based security solution in particular is a critical area which has been the key focus of our attention. A strong emphasis must be placed on cybersecurity and defence to secure resilience and preparedness and, in particular, enhance situation awareness. This will facilitate a better tackling of vulnerabilities and prevent threats caused by the use of emerging technologies. So the possible use of AI to improve cyberoperations' capabilities in the Member States is also taken into account.

Now, it goes without saying that projects on AI and cybersecurity need to be implemented in the most ethical manner. Ethics procedures are standard and have a long tradition in the Framework Programme for Research and Innovation. A procedure for ethics screening and assessment of all R&D projects is enshrined in the EDF Regulation. As I just said, it is modelled along the well-established process applied in the EU Framework Programme for Research.

So, concerning AI in general, as you probably know, the Commission intends to present a proposal for a horizontal legal framework. It could include a number of elements, a risk-based

approach with mandatory requirements imposed in particular on high-risk AI systems of particular concern. For such high-risk AI systems, mandatory requirements could include, for instance, the use of high-quality training data which respect EU rules and values; record-keeping of relevant information in relation to algorithms or programming; provision of information on AI systems' performance; elements securing the robustness and accuracy of requirements; and, of course, finally, human oversight.

Now, turning to this important question of the so-called lethal autonomous weapon systems (LAWS), the EDF Regulation requires that the R&D projects funded comply with all relevant international, Union and national laws, as well as with the ethical principles that are reflected in those texts. During the trilogue negotiations on the EDF Regulation, Parliament insisted that the EDF Regulation specifically prohibit the funding of actions related to the development of such lethal autonomous weapon systems allowed without the possibility for meaningful human control over the selection and engagement decisions when carrying out strikes against humans. So, with this provision, it is very firmly enshrined in the EDF, and the Commission will attach great importance to ensure that all R&D projects selected for funding in the EDF are ethically sound. The EDF Regulation foresees an ethical screening, as I said, an assessment procedure of all fundable projects, including R&D projects involving emerging technologies such as AI. We therefore have to screen all projects from an ethical perspective before funding them. Thank you very much for your attention.

1-012-0000

Anja Dahlmann, *Head of Project – International Panel on the Regulation of Autonomous Weapons (IPRAW), German Institute for International and Security Affairs***.** – My remarks are largely based on the work of the International Panel on the Regulation of Autonomous Weapons (IPRAW), which is an interdisciplinary network of researchers, but overall the views are my own. I will focus on the concept of human control, which is at the core of any regulation of AI-enabled weapons and on a respective international regulation.

First of all, why human control? New technological capabilities, including AI, allow for further automation of a targeted process, especially the increasing speed of warfare, is the biggest asset, as well as the challenge of weapons with autonomous functions. Militaries are preparing to fight at machine speed. Of course, a high degree of automation is not problematic in every context, and many military processes are automated already. Also AI-enabled assisting systems can benefit military decision-making. There is, however, always a need for human control. It is necessary to fulfil operational requirements, to keep legal accountability, to follow the principles of international humanitarian law and for ethical reasons such as human dignity.
But what is human control then? We've heard quite a bit about this today already, and in the understanding of IPRAW, the very minimum requirements for human control are the combination of situational understanding and options for intervention of a human operator. Those elements have to be enabled by design and maintained during use in the targeted process. How those requirements are to be implemented depends on the operational context. Multiple variables contribute to this. Such factors are, for example, the presence of civilians, the likelihood of dynamic changes in the theatre, the type of target, the options for precautions and alternatives, and the purpose, meaning is it defensive or offensive.

All those factors and more define the adequate type and level of human control in a given situation. Due to this myriad of contributing factors, a one-size-fits-all solution for control is unlikely. So how are we to regulate human control? The lack of a fixed formula for human control is a challenge for the norm-making process because an international treaty might not be the best option to capture the necessary level of detail. Therefore, if states – for example in the framework of the Convention on Certain Conventional Weapons (CCW) – wanted to install an obligation to maintain human control, I would recommend something like a 'treaty-plus': a

treaty creating hard law around some general requirements, plus several more dynamic soft-law measures, like best practices and commentaries.

Ultimately, that would create a de facto prohibition of autonomous weapons in most if not all cases, and limit their development substantially. The European Union can play a role in this law-making process in several ways. Parliament's resolution of January of this year was a great step towards that and lists quite a few elements and baselines towards human control. Furthermore, a common position, as called for in the resolution, would be an important step towards an international regulation. There, Member States could define their understanding of human control and show how it might translate into national and international law.

The inclusion of autonomous weapons from the European Defence Fund sends an important normative signal. Further elaboration and guidance could also benefit the CCW deliberations. In the CCW, EU Member States show a certain consensus on the concept of human control, but most shy away from a legally binding protocol. I do understand their concerns, but if even the EU Member States cannot find common ground, I'm quite sceptical for a forum like the CCW.

Overall, the EU has already taken important steps towards the establishment of a concept or even norm of human control, but should not stop here. It should contribute actively and in a coordinated manner to the norm-making process on various levels.

1-013-0000
Chair. – That concludes our first round of contributions from the panellists. We shall now start the debate proper with our committee members. I would again kindly remind committee members to be specific about the panellists to whom they wish to address their questions.

1-014-0000
Radosław Sikorski (PPE). – I have a sort of question to Elizabeth Minor from Stop Killer Robots. When I lived in the US in Washington, I used to go to a place called College Park, Maryland, which was the US's first military airfield where they tested very early aircraft. And there was very interesting documentation there showing that people said: there is, of course, the idea of putting a machine gun on top of one of these machines, but we would never do that. And then we know what happened. I suggest to you that your mission must include the perspective of our potential adversaries, because if our adversaries are to use these systems, we will be forced to use them, too.

Secondly, I'm sure you are aware of a brilliant British movie called Eye in the Sky, which I can tell you as a former defence minister, very realistically shows the dilemmas in overseeing a military operation that includes armed drones. But to my mind, that film shows the reality that, actually, humans are not that good at surveying such operations and I don't know what the solution to that is.

And lastly, I would be very worried about the fusion of artificial intelligence in the military field plus quantum computing, because apparently quantum computing means that all existing ciphers would be broken. And that, of course, opens the possibility that someone using a quantum computer could turn AI-driven systems against us, against their owners, which, of course, is as old as warfare. But what I'm worried about is that that's a contest between the US and China and we as Europe are not even in it.

1-015-0000
Elizabeth Minor, *Advisor, Article 36 NGO***.** – Hi, thanks for the question. On your first point about the perspective of potential adversaries, that's a good argument, really, for multilateral standard-setting and the negotiation of an international treaty. And in the absence of countries that are developing these weapons systems being willing to negotiate at present, it's still important to start setting those norms to move the conversation forward and influence behaviour going into the future, really, before it's too late. And there's a great argument from an

international security perspective to bring people to the table and try and stop an arms-race dynamic which otherwise is in danger of developing and maybe is already here.

On the point that humans are imperfect in our decision-making, for sure, that's true. But I feel that with advanced computational techniques and these new technologies and automation and AI, they reproduce human dynamics, human biases, human ways of going about things. I don't think we should put too much faith in technology as being somehow better than human beings, they are tools that we use, and therefore I don't think we should be over-optimistic about that.

The last question, I'm not sure if I caught the end of it, but I think your point was that Europe isn't necessarily in the kind of high-development end of technologies in quantum computing and certain techniques there. I think that Europe, as I was saying in my presentation, is very well placed to be a leader on standard-setting and thinking through these issues and influencing other partners and their general behaviour in the world. And that's the path that Europe should be trying to pursue.

1-016-0000

Rasa Juknevičienė (PPE). – This is really a very important topic and important because it's about our very near future, of course, about current days, but about the very near future. And my question is maybe for the first speaker from NATO, because myself, I see that artificial intelligence is the area in which the EU could and should work together with NATO in defence. Without that, I think our adversaries will go forward, and speaking about international agreements, I have many doubts when we see Russia today. They are, of course, more and more out of international agreements or they are not fitting to them or they are out of them. So it's really a very important issue and do you agree that working closely with the transatlantic partners is mutually beneficial and good experiences should be shared among partners to avoid the duplication of effort and to progress faster in the field of artificial intelligence? That also includes coordination of actions in implementation in the defence sector with NATO and strategic partners.

1-017-0000

Mircea Geoană, *Deputy Secretary General, NATO***.** – I would move the discussion a little bit beyond current capabilities in the EU. Of course, we know that in NATO we have 30 countries, 30 allies, and for us keeping North America and Europe together when it comes to new technologies is paramount for two reasons.

Today, as we speak, North America and Europe – the EU plus the other non-EU countries in Europe – still represent more than 50% of global GDP, and we represent today something close to 60% of defence spending in the world. We still have, out of the first 40 universities in the world, I think 36, 37 based in the political West.

I'm looking also to the depth of our financial markets, to the fact that our open societies are more conducive to freedom – freedom of thinking, freedom of innovation, and also the freedom of free speech. The fact that our citizens are actively engaging on the ethical and political and moral dimensions of new technologies is something which I think is healthy and not counterproductive. If I add to North America and Europe, NATO and the EU, and the US and Europe, our like-minded democratic partners from all over the world – from Australia, from New Zealand, from Japan, from Korea, from Israel, name it – I see a conglomerate of democracies around the world. Because as our colleague from the US, and as the report of the National Commission on AI, has said very, very clearly, we are also looking at AI new technologies in a way as part of a global competition for the commanding heights of ideas and for alternative propositions of how human society should be organised.

I'm not saying we should gang up; I'm not saying we should create coalitions or go back to Cold War mentalities – just the opposite – but I do believe that if we have still, in the world,

the dominant voice us democratic nations, us in Europe, us in North America, us around the world, then this is the time to shape a global system of governance, including on the responsible use of AI, also when it comes to defence and security. This is something I think all of us should do. Nobody's trying to say 'here, from NATO'. I come from Romania, like Dragoş. I'm a citizen both of the EU and of NATO. I believe in both with the same intensity, with the same love.

I'm not saying that we should try to use the power of regulation in the European Union only as a tool to enhance strategic autonomy or more economic, ideological development in Europe, which I think is something Europe should do. I also believe we have to join forces with like-minded nations and national parliaments and the European Parliament and our public opinions and to shape the debate and also to engage in negotiations with ones which do not share our values.

We are still the dominant force for good in the world. We are still the most important technological and economic and financial actors, but competitors are coming from behind. As the report of the US Congress on AI says, in the next decade China could overcome even the most advanced NATO countries, which is the US and UK and others in Europe. So I think the time is now to join forces, to talk amongst each other and together – together and not separately – and get together in order to shape the global conversation and a system of norms and rules around the world.

If not, as Radosław Sikorski said at the beginning, we will be in a situation of competing with authoritarian regimes that have no limitations in basically using and abusing these technologies in order to surveil their own populations and use them in a malign way – from cyber to hybrid, from AI to robots – in a way that will compel us to go and defend ourselves.

So I think the time is now for common action. NATO and the EU, the US, North America, Canada and Europe, should be the dynamo of a global conversation on this very topical issue.

1-018-0000

Brando Benifei (S&D). – Chair, artificial intelligence and related technologies have surely constituted a turning point in the security and defence sector.

As Parliament stated in the report on ethical aspects of artificial intelligence, use of these technologies must respect the applicable legal regimes, in particular international humanitarian law and international human rights law, and must be in compliance with Union principles and values.

The EU institutions recently reached an agreement on the recast of the regulation on EU export controls on sensitive dual-use goods and technologies. An agreement we have long been waiting for and which will, finally, include among the products subject to restrictions cyber-surveillance tools, such as biometric detection software, that have been produced in the European Union.

Tools that, regrettably, have been used in the past by authoritarian regimes to control and repress their opponents. I would like to ask Mr Arbault therefore how the regulation's new enforcement coordination mechanism will be able to ensure its uniform implementation, avoiding the problems of the previous export control regime?

And then a question for Gilman Louie: we have read with interest in recent months about the growing calls for an export control regime along these lines in the United States too. Could you update us on the situation, and in particular, how do you see matters developing with the new administration?

1-019-0000
François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – It's very important to keep in mind that the EDF will fund the research and development phase of the products which will be screened and assessed against ethical standards. But the funding is on the R&D part. So the Union, the Commission, does not procure the final product so our own products, or whatever is the result of the projects funded under the EDF, will be integrated or purchased by Member States as part of their armaments policy. And Member States in the use of such armaments systems, let's say, have the responsibility to comply with all the commitments that they have taken under international law and national law. So we are doing our part when it comes to the screening on ethical grounds as per the provisions of the EDF. But the Member States remain fully responsible for compliance with any applicable set of laws in the context of the use of those systems.

1-020-0000
Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI)***.** – The National Security Commission on AI is a recommendation body. Both the US Congress and the Executive Branch is reviewing our recommendations, but they have been taken very seriously.

On export controls, particularly around AI, we realise that a lot of AI is open-sourced. It is done in open science and we can't regulate the openness of those technologies, but there are underlying technologies you feel very strongly that should be regulated and controlled and we need to be in coordination with our European and other allies on these controls, particularly around technologies that directly affect the capabilities of AI such as semiconductors. We made very specific recommendations to restrict and limit the flows of critical technologies that could give our competitors a capability to compete with our systems in a way that could be used for military purposes.

I also think that is critical for Europe and the United States and like-minded democratic nations to put very tight controls around autonomous systems and make sure that these systems do not fall into the wrong hands and into the hands of non-state actors.

1-021-0000
Sven Mikser (S&D). – I should like to put my question regarding lethal autonomous weapons systems to Mr Arbault and Mr Louie. This House, the European Parliament, has repeatedly expressed a sense of urgency about advancing the international regulations regarding lethal autonomous weapons systems. Many speakers said that it's imperative that the European Union and the US work together on this. So I would like you to elaborate a little bit as to where you see major similarities and differences between the current European and American approaches when it comes to moving ahead with building this international regulatory framework.

And secondly, as a platform or forum for these discussions, the Convention on Certain Conventional Weapons has been mentioned and has been used previously. But originally this convention was designed to deal with two particular categories of weapons: those deemed excessively injurious and those that do not sufficiently discriminate between combatants and civilians. And AI-enabled systems and lethal autonomous weapons systems, in particular, both pose different legal and ethical dilemmas. So, what do you see as the proper forum or format for advancing those negotiations and discussions regarding the international regulatory framework?

1-022-0000
Pieter Elands, *Program Manager, Unmanned Systems, TNO (Dutch Research Institute)***.** – I actually must say that I am not participating in these international discussions and so I really cannot comment on this question. For me, one important remark I want to make is that considering meaningful human control, which is discussed at these occasions, I think it's very important that we all try to find something, establish what meaningful human control is and get

agreement on it, because we are talking a lot about meaningful human control as an essence of regulating autonomous weapons, but nobody knows what it is and how to achieve it.

1-023-0000
Chair. – Before I give the floor to Mr Louie, perhaps, Mr Arbault, you would like to very quickly try your hand at answering the question? I think the Commission's perspective would also be very interesting here.

1-024-0000
François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – As I said, we have very clear provisions in the context of EDF, so when it comes to the funding of research and development, which means on AI, we proceed to that very thorough screening and assessment. So that's one thing. But when it comes to, again, let's say acquiring and using or exporting systems, this is really the responsibility of Member States, which have the obligation to comply with all international, Union and national laws. This being said, as we know, the issues around the laws are discussed within the group of government experts – the CGE – within the CCW. So there is an international forum which addresses this issue, which involves all UN member states but also NGOs, industry, military experts. So I will say that this is certainly the right forum where countries and member states can discuss those issues, but when it comes to where we are acting in terms of the EDF and the support to innovation in the field of AI, we are basically screening against the provisions of the EDF.

1-025-0000
Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI)***.** – Thank you for the question. I think it's important for the European coalition and the United States to move forward on an active dialogue on these particularly important subjects. One of the recommendations that we made at the National Security Commission for AI is to move forward on a strategic dialogue on emerging technologies with our EU colleagues. We think these kinds of systems are critical.

Let's start with things that we are aligned with. We are aligned on the issues around any kind of autonomous systems that use AI must comply to international human standards, and that standards must ensure responsible, safe, ethical development as well as use. Humans must determine rules of engagement and goal-setting, while commanders and operators must account for the deployment of AI-enabled autonomous systems.

In the US we strongly believe that it is important that we, together with our European colleagues, set very high standards for not only the development of these systems, but for the testing of these systems, as well as the frameworks around the use and deployment of these systems. Where we may differ today is on the issue of whether or not using a banned framework is the right framework. We have some major concerns given the difficulties of actual inspection and the fact that with AI software a system could look perfectly safe, but you're one software upgrade away or a nation could put software into a system that's not viewed as autonomous and AI-controlled to suddenly become AI-controlled.

So I think that Europe and the US could work together both on the research and development track as well as in the enforcement track to start building new tools that will allow not only for safer use of these systems, but also the enforcement of any treaties or any sorts of regulatory environment that come down the road over the next periods of years as these systems come online.

1-026-0000
Svenja Hahn (Renew). – Many thanks to today's speakers for sharing their expertise with us. It truly is a very sensitive topic that we are discussing today. In recent years, the political debate has revolved around the notion of banning autonomous weapon systems. I'd say there is a broad consensus here in Parliament that we don't want any fully autonomous lethal weapon systems

that are beyond all human control – wars are terrible enough as it is! We should therefore be exploring ways of preventing further dehumanisation of warfare.

We're all well aware of the risks inherent in the use of autonomous weapon systems. But I believe we need a highly nuanced debate, as not every degree of automation will automatically lead to dehumanisation. Let's not forget that automation in weapon systems is nothing new: for decades, partly automated systems, such as the Patriot System or Israel's Iron Dome, have offered us a high level of protection. That is why I believe it's important to keep an open mind. We need to stop and think about categories we can explore.

I don't think any of us wants self-determining weapons that do what they want without human control. How, then, can we develop a nuanced approach – one that doesn't involve banning systems that protect civilians and soldiers? We do not want a knee-jerk blanket ban that might then allow others, who do not share our ethical values and principles, to do as they please.

I therefore have a few questions for Anja Dahlmann from the German Institute for International and Security Affairs. Ms Dahlmann, do you believe it would make sense when calling for a ban on lethal autonomous weapon systems to distinguish between offensive and defensive systems and, if so, how should we define these two systems? Or is there another distinction that would be more pertinent in your view? And at what degree of system autonomy might you draw the line for any ban? Is it even possible to measure and legally define this degree of autonomy? Thank you for your answer.

1-027-0000

Anja Dahlmann, *Head of Project - International Panel on the Regulation of Autonomous Weapons (IPRAW), German Institute for International and Security Affairs***.** – Thank you, Ms Hahn. I'll reply in German. It is not easy to say precisely where we can draw the red line with these systems. Therefore, my recommendation would be to introduce a requirement for human control, rather than seeking to define what a fully autonomous weapon system is or anything like that, since this, as you said, opens up a whole new can of worms. Because the thing – or rather the problem – is that the appropriate level of human control depends on the operational context. For example, missile defence systems can certainly be automated more than systems that have to distinguish between civilians and combatants, for instance. So, there are no hard-and-fast rules.

Certainly, the purpose of the weapon is a factor in the equation, but then it also depends where the weapon is deployed. So, if we consider missile defence systems, these work marvellously on ships. But as soon as the ship comes in to port, the context changes completely, and they should be deactivated. Automation would be problematic here.

This is why I would urge you to introduce a human control requirement, where human control means reading a situation, planning and determining the scope of intervention, depending on the operational context. It won't be easy, but I believe legislation is the only meaningful and comprehensive approach.

1-028-0000

Alessandra Basso (ID). – Chair, I would like to thank all the speakers for having shared these interesting thoughts with us.

Interest has, rightly, concentrated on the question of the use of artificial intelligence in the military sector and I understand the necessity, let's say, the interest that more or less everybody has displayed concerning control and final control being in the hands of a human.

The technology involved in artificial intelligence is a technology that we can define as soft somehow because, as far as cost is concerned, it can be implemented even with limited amounts of investment.

I was very impressed when I saw the short film *Slaughterbots* inspired by Professor Stuart Russell, who teaches artificial intelligence at Berkeley. This short film, which is a science-fiction one, showed a future which, however, is not, I believe, so far distant, in which small drones operated by artificial intelligence were capable of automatically selecting targets to kill based on just facial recognition and an analysis of the data of potential victims who, for example, were being hit, those who had posted a particular hashtag on social media, and Professor Russell stressed how we do still have time to act but that the window to do so is closing.

I have two questions that I think several of the experts could answer, otherwise I will address them to Ms Minor and Mr Louie. We say that controlling the applications of large firms and companies is both possible and obvious, but doing so becomes much more complex at the level of small enterprises or informal groups. What, then, could stop a paramilitary or terrorist group, in a not too far-distant future, from using a drone with facial recognition to hit a politician or a human rights activist, and just as there is a ban and control on, let's call them 'conventional', weapons, is it possible to think of a (...) that would render military use of artificial intelligence complex or impossible also at the level of small organisations that can evade controls?

1-029-0000
Elizabeth Minor, *Advisor, Article 36 NGO***.** – A note on companies and industry. Many companies involved in AI development at the moment in the private sector actually would like to see a regulation internationally in this area to make sure that their work isn't misused and that they are not contributing to dangerous developments. So, again, an international treaty would be very helpful for business in this area.

About the possibility of an international treaty, reflecting on what some others are saying. Not all treaties have verification protocols in disarmament, none have universal membership, but I think no one's arguing against other pieces of international law. So I think it's still very important to set a strong, clear international legal standard in this area. As Mr Louie was saying, this isn't a case of particular bits of hardware, so this proposal for a positive obligation on meaningful human control as a core of a Treaty obligation is very important, and it will be principles, rather than prescriptions, as well as prohibitions on certain areas, that are particularly unacceptable.

I think the Members talking about the use of facial recognition to then deploy force automatically on people shows a real problem in this area relating to human dignity and also issues of bias and targeting and that's why we're also arguing for a prohibition on systems that target people in international regulation.

1-030-0000
Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI)***.** – Yes, we agree that it's important for us to have strong regulation that prohibits the use of these kinds of technologies in the situations where non-state actors, irresponsible states or individuals would have access to these technologies. Unfortunately, the technologies described in that video are readily available – if not today, they can be developed within a very short window. It's important for the European Union and the United States to work together on counter-technologies. There are many start-ups, as well as existing defence companies working on anti-drone technologies, technologies that are also used to determine if any of these systems are in operation. I think we need to do a lot more work. These kinds of systems are very difficult to defeat. But I think there's an opportunity for collaboration between advanced nation-states to take these kinds of weapons off the table in terms of their effectiveness.

1-031-0000
Susana Solís Pérez (Renew). – My question is for Mr Arbault: we have seen today that artificial intelligence is of crucial importance to the European defence industry, and you have said that it can have a great many benefits for the armed forces. But when we look at the Member States' 21 national artificial intelligence strategies we see that very few of them relate to the military implications of artificial intelligence and, although they cover many issues, most of them also ignore defence.

Do you think the European Union could play a far more prominent role in encouraging Member States to think more about the military implications of artificial intelligence? And what is the Commission's plan to harmonise strategies and increase Member States' interest in defence applications? For instance, should the Commission draw up a coordination strategy which outlines areas in which a joint European commitment would be particularly useful, such as shared systems for training algorithms, and also draws red lines, as we have seen in the area of the development and use of autonomous life-support systems? Do you think such a strategy for artificial intelligence would be needed?

1-032-0000
François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – As I said earlier, AI has a huge potential and it can go in all sorts of directions. And of course, there are many benefits, as you mentioned, for the armed forces in terms of protection, information superiority, protection and decision-making on the battlefield. So I think in regard to your specific question, I think the EDF and the priority-setting in the context of the EDF work programme that we will adopt, I mean that Member States will adopt every year, is the place where Member States will actually consider the most promising potential of AI, so there might be indeed a focus on those areas where the uses of AI in the defence sector are possibly less controversial, but also very valuable in terms of protection and efficiency of operations. So it's really a matter of conversation between the Member States and the Commission, of course, on how to define the right priorities in order to tap the potential of AI to the best possible extent, while avoiding those areas where we don't want to see undesired developments taking place.

1-033-0000
Anna Bonfrisco (ID). – Chair, my thanks to Ms Loiseau and all the speakers, but my questions are for Mr Gilman Louie.

Mr Louie, my compliments on your career and your commitment to spreading knowledge. I have read the document by the National Security Commission on Artificial Intelligence and I found it articulate and sound, really difficult to find its equal here on the old continent.

First of all I join with all those who say that, in digital transformation, we have the right to be human and stay human and so look after our humanity. I would like to ask you, therefore, to consider my questions through the lens of a holistic approach to security, knowledge and the applications that are being developed on use of artificial intelligence.

The first point concerns innovation in defence and hence military interoperability, political cohesion and resilience. Artificial intelligence will change the battlefield of the future, I definitely think so, so can you guide us in this future in order to understand and define the technological potential of artificial intelligence?

A second subject concerns the democratic future of artificial intelligence – because the technology can boost authoritarianism and erode democracy – since there is increased geopolitical rivalry in today's environment. This means we will have a clash of civilisations in a near future and if so, what elements will characterise this?

Finally, cybersecurity, also in light of the recent attack on the United States; what would be your main recommendations in this field, both legislative and regulatory, to the European Union and its Member States, bearing the digital transformation in mind, regarding what could happen, the damage, and how we can be ready to respond?

1-034-0000
Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI)***.** – Those are all the right questions, by the way, and I appreciate the questions. Let's start off with the innovation of AI to support humanity.

AI is a tool, it's an amplifier. Responsible nations, democratic nations, can use AI to assist the progress of humanity in positive ways in terms of improving the quality of life, drug discovery, protecting our nation-states, to ensure individual freedoms. I particularly point out the importance around the use of AI to ensure things like civil rights and privacy, of which Europe has taken the lead, and we think that Europe can continue to take the lead in these particular areas of research in terms of thinking through civil society. So in the United States and on the commission we are looking forward to working with the EU on these particular issues.

Interoperability is critical. If we have systems that are dependent upon information-sharing and coordination as part of protecting our unions against nation-states and other threats, then we can't afford to have seams. Having systems that are not communicative, do not use the full availability of the range of sensing and information could lead to poor decision-making and could be exploited by adversaries.

I think there is a democratic future for AI and in this kind of global competition of values, each nation-state has different sets of priorities; some of our competitors prioritise the importance of security and harmony over individual rights and freedom of speech. It's very difficult to program AIs and train systems with data that don't mimic those values, and I think for us, having those standards as democracies, it's critical to say what are acceptable uses of these technologies and what are not acceptable uses of these technologies. Facial recognition is a great example. It has a lot of value, but it also can be a dangerous no-person's land if it's used to further discrimination or target subpopulations.

As for the sack of civilisations, I think it's important for all nation-states, including our competitor states, to have active strategic dialogue so that we do not misinterpret each other's actions or deployments of these algorithms and these technologies.

And finally, on the cyberside, particularly in light of recent attacks such as the SolarWinds attack, we believe the appropriate use of AI could have in fact been very helpful in determining whether or not these attacks were taking place and even coming up with mitigation strategies. Unfortunately, across our nation-states and between governments and commercial populations in the civilian world, we do not have the sharing frameworks in place that would allow us to use these kinds of systems to protect our cyber-infrastructure. There's work to be done.

1-035-0000
Alexandra Geese (Verts/ALE). – I have a specific question for Mr Louie. You mentioned among the threats to national security by artificial intelligence specifically AI tools to disseminate malign information. Would you like to elaborate a little bit on this? And what are the measures you would recommend against this? You already mentioned data protection, but I think you can certainly go into more detail and I would like to give you the minutes missing from my speech for my part for your answer.

1-036-0000
Gilman Louie, *Commissioner, US National Security Commission on Artificial Intelligence (NSCAI)***.** – I'm more than happy to answer that question. I think AI could be a powerful tool to our adversaries in isolating down, in real time, messages that are resonating and accelerating

disinformation or information that can be sensationalised. We know from research that sensationalised information, and even lies, spread at faster rates than truth, which is challenging. And automated systems that can perfect language and attitudes and reinforce the worst in us are also very dangerous and can be used by our adversaries in dangerous ways.

But I do believe AI can also solve some of the problems and help in early detection of this kind of misuse. It is our view that if we think of malign information like the way we would think about a virus, we would be able to figure out where was ground zero of a piece of information. We could put provenance around these accelerated misconceptions or messages of hatred. We can see the super-spreaders by what we would call in the cyberworld influencers and how networks use those influencers as a way to accelerate these kinds of information. We will be able to potentially expose false information being spread through false accounts.

Now, both the technology sectors and nation-states need to work together and figure out frameworks that make information more transparent as a way for humans, individuals, to make better judgement as to the quality of the information they are receiving and whether or not an algorithm or group of individuals are trying to manipulate information for ill-gotten gains.

1-037-0000

Markéta Gregorová (Verts/ALE). – I think my question is probably most directed at Mr Arbault. For me, there is one very important question on the table, but first, a little bit of background. As you know well, the European Defence Fund will soon enter into force and the European Commission will be allowed to implement it, which means that it will receive proposals for co-funding military research and development projects. In order to well respect the Regulation, the Commission needs to operationalise concepts laid down in the legal text. As regards AI and autonomous weapon systems, there is one very important framework described in Article 11, point 6 of the Regulation, which says that weapon systems without meaningful human control cannot be co-funded by EDF. The Commission will probably be the first executive or governmental administration in the world to be obliged to operationalise these key concepts as regards AI and autonomy in military technology by generating precise criteria and benchmarks. It needs to operationalise meaningful human control, early warning systems and countermeasures for defensive purposes. So I would be interested in how the Commission will generate such criteria. Will it seek help by external experts? And if so, which ones? From what sector? And will the Commission communicate to the Parliament – which has had a very clear position on autonomous weapon systems since 2018 and which is responsible for this legal language in EDF – a draft set of criteria and enter a dialogue? Thank you.

1-038-0000

François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – I think there was a slight interruption, but I think I got the gist of the question. Indeed, we have this very clear prohibition, this prohibition on loads without any meaningful human control, we will have to apply that provision. As I said, we will very carefully screen and assess the proposals. Any proposals not meeting the tests set out in the regulation will be excluded from funding. That is very clear.

We will issue guidance for applicants, but also for the independent experts, experts in the field of ethics that will help us actually carrying out that screening and assessment. So moving forward we will have to further specify, if need be, how to actually operationalise the application of that test. But we will provide all the necessary guidance for applicants to figure out what they have to avoid putting in the applications and be sure that we really rely on very knowledgeable experts in the field to assist us in actually making the findings that would lead to the exclusion of any project not complying strictly with the tests set out in the EDF.

1-039-0000

Adam Bielan (ECR). – First of all, I would like to thank all the experts for their contributions. My questions will be mainly directed to Mr Louie. In your capacity as Commissioner in the

National Security Commission on Artificial Intelligence, I would like to ask you about transatlantic cooperation on AI in a security and defence context. It seems the US and the EU are on different paths when it comes to regulating artificial intelligence and have distinct points of view on data-sharing restrictions and liability agreements, but there is also a need for greater cooperation to face strategic competitors, which can also challenge our values. In your view, what are the obstacles to enhanced transatlantic AI cooperation and where could we find a greater understanding and common ground? You partly addressed this before in responding to Mr Mikser's question but still I think it is very relevant.
And second, in your commission's report published this week, it is stated that, '[i]f the United States wants to fight with AI, it will need allies and partners with AI-enabled militaries [...]. Uneven adoption of AI will threaten military interoperability and the political cohesion and resiliency of U.S. alliances'. Following on from Ms Bonfrisco's question, how would you evaluate the risk of de-synchronisation of defence and intelligence activities between the US and the EU? In your opinion, what could be done to prevent the growing divergence in this area?

1-040-0000
Gilman Louie, *Commissioner, U.S. National Security Commission on Artificial Intelligence (NSCAI)***.** – First, I think it's important to start with dialogue. The new Biden Administration has stated in its first 100 day plan that it is important for us to reach out to our allies and begin to have dialogue. This is clearly a topic where we all need to put our best experts together to solve real world problems, not just problems around concepts.

Let's start with data sharing. In the nature of data itself, both Europe and the US understand the importance of data sharing and data, particularly when it comes down to machine learning and artificial intelligence. Understanding the principal frameworks of what both the US and the countries within the EU consider acceptable data and setting-up data standards that will comply with both EU member nations and with the United States is critical, I think. Those datasets that will train up our systems that would have to operate on a battlefield or in a military setting starts with that data. I think it's very important that we put working groups to solve those sorts of problems, not just where on the provenance of that data, but to make sure that data does not have built-in biases or weaknesses that will mistrain our systems.

I think the second thing in terms of AI-enabled systems is coming to mutual agreement as to what the standards are on what meaningful human control is, and what the conditions are in which these systems should be allowed to operate. Meaningful human control is important, but meaningful authorisation and meaningful responsibility of these systems are also very important. Those frameworks need to be discussed, and with dialogue.

How we use these new technologies against systems that we may encounter is particularly important. I think we all recognise that decision times because of technologies that don't have anything to do with AI, as in the case of stealth electronic warfare technologies and cyber, hypersonic, energy and beam weapons, all are compressing the decision timeframes in which actors and responders get to make meaningful human decisions. Hence this concept of the 'person in the loop' is collapsing and being replaced by 'meaningful human control'. We have to define what that really means in the operational context.

So there's a lot of work between NATO, the EU and the United States that needs to be done, but it starts with dialogue. That's why again we're proposing to have strategic dialogues on emerging technologies as a high priority between our member nations of NATO as well as across our transatlantic relationships.

1-041-0000
Alexandr Vondra (ECR). – I think it's important we all understand we are lagging behind China, behind Israel, behind India, behind the UK, of course behind the US, so I think that the EU has this same problem, a lack of political will. And it's up to us, the politicians, to fix that.

Secondly, on over-regulation, listening to many voices here I am a bit sceptical because this tendency of the EU to portray itself as an entity obsessed with the rules instead of the results does not lead me to the conviction that we would be able to match them. You know, we are trying to build some kind of a lighthouse or Garden of Eden here, but the Russians, Chinese are not going to follow us. But that's just my sceptical view, certainly it's about the resources, and here is my question both to Mr Arbault and Mr Geoană: how much would the EU have to raise to match China, let's say in five years, if the EU is going it alone? That's to Mr Arbault.

To Mr Geoană: if we do this together with the United States and Canada inside NATO, you know, how much would we have to raise additionally on the yearly level not to allow China to become a superpower here?

1-042-0000
Chair. – Mr Arbault and Mr Geoană, I will give both of you the floor. I will already sacrifice my own concluding time so that we can fit into the current planning, but for all the remaining speakers, try and be compact. Mr Arbault, you go first.

1-043-0000
François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – I shall be very brief. I am talking from the technological perspective and here we are committed to make sure that any research or development project that is funded will entail a meaningful human control. This is the strict minimum as per the expectation of the co-legislators.

When it comes to strengthening the rules applying to the use of weapon systems this is a matter of international dialogue, this is a matter of developing international law, and of course I want to insist on that because I didn't so far. We will take a kind of dynamic approach to that which means of course that we will actually make sure, as rules and laws develop, that the state of the law, the state of the rules, are recognised internationally, will be actually the set of laws that will apply in the assessment that we will carry out. So this dynamic approach guarantees that we will stick to the highest possible standards set out by the international set of laws.

1-044-0000
Mircea Geoană, *Deputy Secretary General, NATO***.** – I am so happy to see you Saša. Let me say just one thing that I believe is critical to this conversation. NATO is a political and military organisation, and in that alliance of ours of 30 nations, 21 Member States of the EU are also allied members – 21 out of 26.

In terms of global defence spending, from the whole of the alliance, EU Member States are spending only 20% of the whole alliance defence budget. So when it comes to an organisation that has inside it politicians and our leaders, that has inside it our military commanders and military leaders, an organisation that is doing defence planning with each of the allies, including the 21 Member States of the EU that are also allied members, every year when we introduce in national defence spending and national defence plans and armament plans, the things that we decide together, and when NATO starts to introduce by design for all allies, all 30 allies, by design – ethical values, rule of law values, international-level values, interoperability by design – NATO is the place to do these things together, across the Atlantic.

I'm not saying that we should not do things in other formats, but this is a political and military organisation and the standards-setting power of NATO is just immense.

Saša, I don't think we should spend much more than the 2% percent of GDP on defence that all allies committed to in Wales. Even today, we can with better spending, smarter investment, make the smart transition from traditional deterrence and defence to the new era of defence, security and war fighting. NATO is equipped and we are doing this as we speak.

We have a NATO summit in a few months from now. One of the most important initiatives of the Secretary General will be to push forward on innovation. So I do believe that NATO and the EU, the US and Europe, Canada and Europe, and all other democratic nations around the world, are just irresistible.
No country alone can face the rise of China successfully, no country alone. We need each other more than ever and I think NATO is the platform of platform on defence and security. NATO and the EU should work in convergence and not in divergence in coping with these things together.

1-045-0000
Chair. – We have three more speakers, one from the EPP Group and two non-attached Members. I will take the questions together and I would kindly ask the panellists to pay attention to the three questions because then they will reply to them in one go.

1-046-0000
Riho Terras (PPE). – Development in the field of innovation technologies and AI is moving rapidly, and the EU needs to act as fast to stay relevant in the global competition. Given that this is a high-risk area, of course attention must be paid to the legislative side as well. We should not over-regulate but still take into account that the subject of the legal regulations is actually a human being.

When it comes to the funding, the EU has a large toolbox ready to support new technologies in the defence sector. There are several promising areas which need to be prioritised by the Commission when it comes to the funding from the European Defence Fund. In particular, I would like to point out the growing need for AI data centres, and AI under it needs training with a lot of data in order to become reliable. Such data centres are inevitable if the EU wants to develop AI solutions and be competitive in the global arena. Consequently, such data centres will be crucial for the EU capability development and for providing the EU military industrial base with the necessary data sets.

So, here's my question to Mr Arbault: what do you think about the need for AI data centres? Has there been discussion in the Commission over it, or has that topic not been considered yet?

1-047-0000
Sabrina Pignedoli (NI). – Chair, the most recent report from Italian intelligence documented attempts to steal data from research centres and firms working on production of COVID-19 vaccines.

The same thing is happening in other European Union countries. These attacks are often conducted using artificial intelligence tools and machine learning algorithms, and behind them lie not just independent hackers and transnational criminal organisations but also groups linked to foreign government structures.

Cyberattacks of this kind will happen more and more frequently, and only with highly advanced artificial intelligence systems will we be capable of withstanding them. One question on internal security but also on defence. The European Union must be cohesive in this too and a pioneer, and I ask, therefore, what initiatives in this regard the EU plans to adopt?

Are agreements with non-EU countries being studied to withstand the threats to cybersecurity, and if so, with which ones? What is the state of play on initiatives to improve, within the

European Union, cooperation between governments, private research centres and universities on the cybersecurity front?

1-048-0000
Fabio Massimo Castaldo (NI). – First of all let me warmly thank all the distinguished speakers that are here with us today. Their insightful introductory remarks are essential for deepening our knowledge and understanding of crucial topics such as artificial intelligence, cybersecurity and cyberdefence. Only if we address the challenges and opportunities that emanate from these domains can we look optimistically at the future.
However, strategic autonomy does not mean going all the way alone. On the contrary, the EU must reinforce its cooperation with mutual and essential partners such as NATO. Therefore I would like to ask NATO Deputy Secretary-General Dr Mircea Geoană whether NATO has devoted *(inaudible)* for power defence capabilities in the defence-planning process? Do you see possibilities for announcing cooperation between NATO and the EU in the capabilities-development process, mostly through more concrete alignment between the NDPP than capacity-development plans (CDPs) and the coordinated annual review on defence, the so-called CARD?

Second, I'd like to ask Dr Pieter Elands what he believes to be the most important characteristic for a counter-unmanned aerial system that would be effective against the malicious use of micro- and mini-drones? We know that the CUAS systems must be scalable for adapting to different environments and that the possibility of countering malicious UAS in an urban environment is much more limited than in an out-of-air mission. Do you think it is possible and effective to focus our efforts on creating the CUAS that can be used in both theatres, or is it better to invest in two different solutions? How do you evaluate the PASC project led by Italy, aiming at creating a CUAS system?

1-049-0000
Chair. – It's been much more than one minute. So, we have three responses from three different speakers. We have five more minutes, and I thank the interpreters for giving us the extra five. Two concluding remarks from the AIDA rapporteur and from the AFET Vice-Chair. Difficult, but let's try – if everyone sticks to exactly one minute. Mr Arbault, you go first and try to fit it in one minute.

1-050-0000
François Arbault, *Director for Defence Industry, DG DEFIS, European Commission***.** – Very quickly, I think on over-regulation it's certainly not our intention to over-regulate AI. As I said, the Commission sees AI as a very promising field. We can tap that huge potential on a positive agenda, but of course we need to also harness the risks, so this is really a matter of a balanced approach. The EU, as I said, is set to actually define a horizontal framework, framing precisely around certain principles to really tap the potential of AI whilst avoiding risk.

It's also a matter of building the requisite infrastructures, and we have programmes to that effect in terms of digital Europe to actually establish the infrastructures that will really underpin tapping the potential of AI. We must also avoid that the potential of AI is turned against us, and indeed we need to invest in cyber-capabilities. We need to be able to have, for instance, C2 clouds.

So this is really a matter of building the infrastructures, defining the principles, tapping the potential whilst really being extremely vigilant on the risks that could be associated with a technology which is as destructive as AI, but we are very much geared towards achieving that objective.

1-051-0000
Pieter Elands, *Program Manager Unmanned Systems, TNO (Dutch Research Institute)***.** – The subject of counter-UAS is a very important one, because the use of drones by non-state actors and others is really growing. We think there's not one single solution – that really it must be a

combination of various different solutions, and that the context very much determines what kind of combination of solutions is being used. As Mr Louie said, there's a lot of effort going on. The cooperation is very important, and lots of this work can also not be discussed in the open. But I cannot underestimate the importance of it. But not really one single solution, so a combination of various different technologies.

1-052-0000
Mircea Geoană, *Deputy Secretary General, NATO***.** – *(start of speech inaudible)* very briefly towards the end. Other than chairing the Innovation Board in NATO, I'm also doing, on behalf of the Secretary-General, NATO-EU a lot. And let me tell you, as an answer to our Italian colleague's question, what we have decided together to engage between NATO-EU on top of the already very rich and dense cooperation in the strategic partnership between our two organisations.

So, we decided to work together on new technologies; on resilience; on space – which has been declared by NATO as an operational domain just one year ago; on the rise of China; and also, I think most importantly, on working together to defend, to reinvigorate and to innovate the international world system of global governance from a democratic and free-world perspective. These are the five things that we decided together, Ms von der Leyen and the Secretary-General Stoltenberg.

I'm doing this every day with the Commission and I'm ready to engage also with the European Parliament, because I was a parliamentarian myself. I'm a politician myself in my former incarnations. I know how important it is to engage with you. So, yes, we can do, and we should do, much more between NATO-EU in any dimension that our leaders will be agreeing upon. I'm all for it – 100% – in this effort to bring NATO-EU ever closer together.

1-053-0000
Chair. – Thank you very much, Deputy Secretary-General, and thanks to all our panellists. It's been a very valuable contribution from all of you. For the closing remarks, which will have to be very short, I would like to hear from both the AIDA rapporteur Axel Voss, and the AFET vice-chair and SEDE member Urmas Paet.

1-054-0000
Axel Voss (PPE), *rapporteur for the Special Committee on Artificial Intelligence in a Digital Age (AIDA)***.** – Thank you, Dragoș. I assume I can continue in German, but I'll try to keep it brief.

With other countries across the globe using AI, we also need to embrace this development. And we need to base our efforts on international coordination, on closer cooperation – including between NATO and the EU. Currently, we still have the influence to make a difference at the global level and our overall aim should be to impose an interoperable system at that level as well. The security structure of the EU must also not be undermined and we should take full advantage of this opportunity to innovate – in this field too.

As we move forward, however, we should also consider the following: research and defence should go hand in hand here, and minimum human control requirements put in place, including ethical screening. Here too it has been suggested that the EU might want to devise rules on human control.

High-risk applications in particular – including autonomous weapons, which are something of a special case – should be matched by ethical guidelines and accountability, covering, in particular, the issues of facial recognition and data centres.

Key to all this is, of course, investment, i.e. money, and here the EDF will prove crucial and we must not restrict its scope.

Cybersecurity was also mentioned, as data must not end up in the wrong hands. Less was said about the quality of algorithms, the quality of data standard testing and monitoring, or the state of the art. I assume this was taken as a given, but these are important concerns which we should also address in the report.

1-055-0000

Urmas Paet (Renew), *Vice-Chair of the Committee on Foreign Affairs(AFET)/Member of the Subcommittee on Security and Defence (SEDE)***.** – Yes, hello and good afternoon. Artificial intelligence-enabled technology has the potential to transform modern warfare, and AI can be used to generate large quantities of fake news, which could, for example, lead to military conflict. And in cybersecurity, artificial intelligence could be used to improve intelligence processing, but it could also be used offensively. Member States have the responsibility to guarantee the defence of their citizens, and that also applies in the case of cybersecurity and AI. However, while cyberdefence remains a core competence of the Member States, nevertheless, due to the borderless nature of cyberspace, it is not possible to tackle the threats and challenges by any one state alone. Member States must cooperate closely, and this is where the European Union can be of help. The EU needs to provide a platform for European cooperation and ensure that the new endeavours are closely coordinated at an international level and within the transatlantic security architecture. Cooperation with NATO is of utmost importance and must continue and increase. The rapid development of emerging technologies, in particular artificial intelligence, only makes it more urgent. Cyberspace enables and amplifies the malign use of artificial intelligence while building a secure common infrastructure and space also for data, provides the EU and NATO with the necessary tools to develop and adopt such technologies. We should not build competing silos but a common approach based on our shared values.

1-056-0000

Chair. – Thank you very much Urmas. This concludes today's hearing as well. Thanks to all members for following us. Again, a very warm thank you to our interpreters for staying with us for the extra time. Thanks also to the technical team for making it happen. We'll see each other at the next hearing, and the full recording of today's session will be available on AIDA's website. Thank you very much and good afternoon.

(The meeting closed at 15.55)