NATO PARLIAMENTARY ASSEMBLY

SUMMARY

OF THE MEETING OF THE

SCIENCE AND TECHNOLOGY COMMITTEE

Saturday 1 June 2019

Music Hall
Bratislava Castle
Bratislava, Slovakia

128 STC 19 E | Original: English | 13 June 2019

ATTENDANCE LIST

Committee Chairperson	Maria MARTENS (Netherlands)
General Rapporteur	Susan DAVIS (United States)
Rapporteur	Matej TONIN (Slovenia)
NATO PA President	Madeleine MOON (United Kingdom)
NATO PA Secretary General	David HOBBS

Member delegations

Belgium	Brigitte GROUWELS
	Damien THIERY
Canada	Joseph A. DAY
Croatia	Nenad STAZIC
	Miroslav TUDJMAN
France	Anissa KHEDHER
	Joachim SON-FORGET
Hungary	Agnes VADAI
Iceland	Arna Gerdur BANG
	Njall Trausti FRIDBERTSSON
Italy	Andrea CANGINI
	Fabrizio ORTIS
Latvia	Aldis BLUMBERGS
Lithuania	Vytautas BAKAS
	Dainius GAIZAUSKAS
	Rasa JUKNEVICIENE
Luxembourg	Sven CLEMENT
	Roberto TRAVERSINI
Montenegro	Obrad Miso STANISIC
Netherlands	Sven KOOPMANS
	Janny VLIETSTRA
Norway	Lene WESTGAARDE-HALLE
Poland	Jozef LYCZAK
Portugal	Bruno VITORINO
Slovakia	Milan KRAJNIAK
	Juraj SOBONA
Spain	Begona NASARRE
Sweden	Karin ENSTROM
Turkey	Hisyar OZSOY
	Kamil SINDIR
	Taner YILDIZ
United Kingdom	Baroness ADAMS
	Douglas CHAPMAN
	Kevan JONES
	Baroness RAMSAY OF CARTVALE
	Andrew ROSINDELL
United States	Neal DUNN
	James SENSENBRENNER
	John SHIMKUS

Associate Delegations

Armenia	Gevorg GORGISYAN
Azerbaijan	Malahat IBRAHIMGIZI
Bosnia and Herzegovina	Nikola LOVRINOVIC
Finland	Tom PACKALEN
	Mikko SAVOLA
North Macedonia	Katerina KUZMANOVSKA
Switzerland	Pierre-Alain FRIDEZ

Regional Partner and Mediterranean Associate Member Delegations

Morocco	Mohammed AZRI

Speakers

Lukas PARIZEK
State Secretary, Ministry of Foreign and European Affairs, Slovak Republic

Jan-Peter KLEINHANS
Project Director IoT Security, *Stiftung Neue Verantwortung* (SNV)

Helena LEGARDA
Research Associate, Mercator Institute for China Studies (MERICS)

Pavel ZUNA
Director of the NATO STO Collaboration Support Office (CSO)

International Secretariat

Henrik BLIDDAL, Director
Ginevra SPONZILLI, Coordinator
Gillian HANNAHS, Research Assistant
Angelica PUNTEL, Research Assistant

I. Opening remarks by Maria MARTENS (Netherlands), Chairperson

1. The Chairperson of the Science and Technology Committee (STC), **Maria Martens** (NL), declared the STC meeting at the 2019 Spring Session open. She welcomed all members and thanked the Slovak delegation for preparing the Session.

2. She delivered some practical notes on registration, moving towards paperless sessions, speakers' biographies, social media, and the agenda.

II. Adoption of the draft Agenda [086 STC 19 E]

3. **The draft Agenda [086 STC 19 E] was adopted.**

III. Adoption of the Summary of the Meeting of the Science and Technology Committee held in Halifax, Canada, on Sunday 18 November 2018 [249 STC 18 E]

4. **The Summary of the Meeting of the STC held in Halifax [249 STC 18 E] was adopted.**

IV. Consideration of the Comments of the Secretary General of NATO, *Chairman of the North Atlantic Council, on the Policy Recommendations adopted in 2018 by the NATO Parliamentary Assembly* [043 SESP 19 E]

5. The Chairperson recognised the *Comments of the Secretary General of NATO, Chairman of the North Atlantic Council, on the Policy Recommendations adopted in 2018 by the NATO Parliamentary Assembly* [043 SESP 19 E].

6. There were no comments from the Committee members.

V. Presentation by Lukas PARIZEK, State Secretary, Ministry of Foreign and European Affairs, Slovak Republic, on *The Future of Confidence- and Security-Building Measures and Arms Control in the OSCE Framework: A Perspective from the Slovak OSCE Chairmanship*

7. State Secretary **Lukas Parizek** began his intervention by stressing how the Organization for Security and Co-operation in Europe (OSCE) and NATO were the cornerstones of the Euro-Atlantic security architecture. Both institutions had been created for the security of the citizens in the Euro-Atlantic space. They were succeeding in making the Euro-Atlantic space feel secure, safe, and stable for its citizens. In 2019, Slovakia held the chairmanship of the OSCE. The Slovak Chairmanship had three main priorities, he underlined. First, it wanted the OSCE to refine the focus on the prevention and resolution of conflicts. A second priority was to ensure the future security of people in the OSCE area and beyond, with a focus on cooperation and hybrid threats. Thirdly, Slovakia wanted to focus on effective multilateralism, he stressed, as comprehensive and inclusive cooperation was essential for security.

8. Under the OSCE's military dimension, the organisation supports the implementation of conflict prevention measures. He stressed that NATO and the OSCE should work together in order to update these measures and follow up on implementation. In this sense, rebuilding trust between international actors was fundamental. Slovakia, he went on, supported structured dialogues as key platforms to ensure trust and avoid disruptions of inter-state relations.

9. He observed that the world had never been a safe place: currently, imbalances in the distribution of wealth, arrogance, ignorance, and social exclusion all contributed to the rise of extremism. As a result, emphasis should not only be placed on military threats. Synergies between the OSCE and NATO should be developed to help face these new challenges. Coordination and information sharing should be prioritised as well.

10. The Chairperson opened the discussion by asking about the current status of the OSCE's relations with Russia. Other questions from participants focused on concrete ideas for enhanced cooperation between the OSCE and NATO as well as OSCE efforts on cybersecurity, social media and information operations, hate speech, and migration flows.

11. Mr Parizek underlined the OSCE was an effective discussion platform with Russia, since every Participating State of the OSCE had the same voice and veto right. The events of 2014 and the ongoing crisis in Ukraine had affected the functioning of the organisation, he admitted, but debates were still central. Moreover, in the Eastern part of Europe, the OSCE continued to be very popular and well-known, and the countries in the region largely recognised the value of its mission. Russia was part of the OSCE, and every security threat should be raised at the OSCE table.

12. The cooperation with NATO, he observed, dated back to the 1990s. Currently, NATO offered protection and logistic support to OSCE missions. For example, the election observation process in Afghanistan had taken place in cooperation with NATO. He observed that both organisations should always find new ways to join forces and support each other to be more effective. With regard to migration, Mr Parizek explained how various chairmanships had made this a priority, including the current Slovakian chairmanship. This topic was mainly addressed through dialogue with Mediterranean partner countries.

13. The speaker recognised how the understanding of security had broadened. Cybersecurity, he added, was a new focus in the OSCE's work. He admitted that the organisation had approached this new space a bit too late. A colleague of Mr Parizek's from the Ministry of Foreign Affairs, **Ambassador Robert Kirnag**, explained the OSCE's cyber efforts. The organisation focused on cybersecurity of states and, thus, not on cybercrime, for example. Important elements of the cyber efforts focused on confidence building measures and focusing on regional cooperation and the protection of critical infrastructure. With regard to hate speech, Mr Parizek underlined how educational OSCE seminars were important tools. They needed to be coupled with tolerance and non-discrimination, too, he argued.

VI. Presentation by Pavel ZUNA, Director of the NATO STO Collaboration Support Office (CSO), Paris, on *NATO STO CPoW (Collaborative Programme of Work) towards Maintaining the S&T Edge*, followed by a discussion

14. **Pavel Zuna** started his presentation by referring to several tasks set out in the 2019 NATO Political Guidance which are relevant to NATO Science and Technology (S&T):

- to maintain the technological edge;
- to accelerate capability development;
- to stay at the forefront of S&T;
- to increase the number of demonstrations of prototypes; and
- to enable rapid transition of technologies.

15. The Science and Technology Organisation's (STO) main goal was to maintain the technological edge and enhance the Alliance's agility, Mr Zuna pointed out. The STO used different business models to deliver on this goal:

- a collaborative business model which provided NATO members a forum to use national resources to define, conduct, and promote cooperative research and information exchange; and
- an in-house delivery business model in the Centre for Maritime Research and Experimentation (CMRE), where activities were led in a dedicated executive laboratory with specific personnel, capabilities, and infrastructure.

16. At the CSO, the core of the collaborative business model comprised several panels and groups which managed a wide range of scientific research activities and supported the organisation's information management needs. World-class scientists, engineers, and information specialists staff these panels, he said. In addition to providing critical technical oversight, these panels also offered a communication link to military users and other NATO bodies. Currently, the Collaborative Programme of Work (PoW) had over 6,000 active scientists, engineers, and analysts working on more than 300 research activities per year. The most active countries were the ones with a strong defence research and industry base, such as Canada, France, Germany, the Netherlands, the United Kingdom, and the United States.

17. Mr Zuna told Committee members that the budget for his office was about EUR 6.6 million. If one combined this number with the national resources put into the Collaborative Programme of Work, more than EUR 500 million were spent annually on NATO S&T. The Programme, he went on, supported nations in building national capabilities and NATO in building NATO-owned capabilities. He mentioned strong cooperation with NATO's Allied Command Transformation (ACT) and the NATO Industry Advisory Group (NIAG).

18. He then described several recent highlights in the CPoW, including on military mobility; big data; maritime unmanned systems; the Allied Future Surveillance Capability; the acceleration of capability development and delivery; and structured partnerships with ACT, Allied Command Operations, and NIAG. Finally, he mentioned NATO S&T's *Tech Trend Report 2018*, which outlined the short-, medium-, and long-term consequences of new technologies.

19. The ensuing discussion was opened by several questions on research on:

- satellite navigation in the High North;
- unmanned aerial vehicles (UAV) including counter-UAV;
- legal, ethical, and moral questions related to lethal autonomous weapon systems;
- hypersonic weapons;
- the value of social media in an operational context;
- NATO STO's financial resources; and
- artificial intelligence (AI) for decision making.

20. Mr Zuna started by saying that scientists and engineers should look beyond current satellite navigation capabilities. For example, he argued quantum science developments potentially offered more precise navigation systems. He warned that China might be ahead of the Alliance in this respect. He went on by outlining the first necessary steps for defence against UAVs, namely detection and identification. He told delegates that researchers were looking for different radar systems to enable detection of UAVs. On the legal, ethical, and moral questions related to lethal autonomous weapon systems, he pointed out that NATO was working on developing policies. At the same time, scientists were working on new technologies to allow the Alliance to maintain meaningful control of systems based on artificial intelligence. On hypersonic weapons, he stressed that some physical limits could not be overcome by NATO nor Russia, even if the latter often issues claims to the contrary. For example, hypersonic missiles operated with speeds and in a level of the atmosphere which made communications impossible. On social media in an operational context, Mr Zuna pointed to NATO S&T efforts to understand hybrid warfare in the Donbas region, upon request by Ukraine. On the use of the STO's budget, he pointed out that his office merely supported the activities and collaboration

between member states and did not finance any research. He concluded by referencing an effort to examine AI's potential for decision-making support.

VII. Consideration of the draft General Report *NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence* [087 STC 19 E] by Susan DAVIS (United States), General Rapporteur

21. **Congresswoman Susan Davis** (US) started the presentation of her draft General Report by highlighting how today's society was becoming increasingly interconnected and how cyber threats were skyrocketing. Networks owned by NATO suffered hundreds of cyber incidents every month, she observed, and intrusions into crucial networks in Allied nations were rising, too. Her report focused on cyber threats going to the core of NATO's *raison d'être*: cyber-attacks which threaten the territorial integrity, political independence, or national security of NATO member states, i.e. cyber-attacks which could lead an Ally to invoke Article 5.

22. Cybersecurity, defence, and deterrence had become an unambiguous part of NATO's core tasks, she underlined. As a result, a sufficiently harmful cyber-attack against an Ally would be considered an armed attack against all, she stressed. In 2018, Allies had reaffirmed their commitment to employ the full range of capabilities to counter cyber threats and had recognised cyberspace as a domain of operations. She stressed the important steps taken by Allies in integrating cyber capabilities into operations. Next to cybersecurity, defence, and deterrence, she stressed how international norms could also become an important addition to Allied cyber strategies. She also recalled NATO's concrete cyber actions, such as the establishment of a Cyberspace Operations Centre, several cyber Smart Defence projects, the NATO Industry Cyber Partnership, and the crucial cooperation with the European Union.

23. She then focused on how states could deter future cyberattacks. The ability to signal retaliatory capabilities and resolve were fundamental. Since signalling was difficult in cyberspace, she highlighted the US doctrine of "Persistent Engagement". By maintaining a continual state of action using cyber capabilities, Allies could gain a strategic advantage, she noted. She finally asked whether NATO was the right institution to be developing collective deterrence strategies and cybersecurity policies, since cyber defence was a national responsibility. And if so, what should those strategies and policies look like?

24. Questions and statements from the delegates tackled several fundamental issues:

- how to make correct attributions of cyber operations and whether states should publicly attribute cyber operations to state actors;
- how to share information between Allies;
- whether NATO was the right institution to tackle cyber issues;
- what the right response would be if Article 5 was invoked;
- how to improve cooperation between NATO and national computer emergency response teams;
- when and how companies and the state should publish vulnerabilities; and
- how developments in the private sector could be leveraged by the public sector.

25. Congresswoman Davis began by underlining the difficulty for certain Allies to share information about cyberattacks they had endured, particularly with regard to how that information had been obtained. She stressed how, with better cooperation, every Ally was better off, but also how it was still unclear how transparent governments should be about cyberattacks. With regard to a credible response from NATO in an Article 5 scenario, no clear rules had been established, she noticed. She observed that question of "how to retaliate without escalation" needed to be answered. Finally, she stressed how, at the same time, the creation

of a policy and overarching structure that applied to every member was very challenging, since national law enforcement agencies would be involved in the process.

VIII. Consideration of the draft Report of the Sub-Committee on Technology Trends and Security *Artificial Intelligence: Implications for NATO's Armed Forces* [088 STCTTS 19 E] by Matej TONIN (Slovenia), Rapporteur

26. Almost all defence experts agreed that the application of AI in the armed forces could impact every domain and level of warfare, stressed Rapporteur **Matej Tonin** (SI). In the report, Mr Tonin outlined some opportunities and challenges related to the application of AI in the defence sector. First of all, he noted, AI solutions could boost the speed of analysis and action and also improve the quality of decision-making. Robotic autonomous systems also offer vast opportunities, he argued. AI would enable robotic systems to do much more than they currently do. These opportunities could force countries to restructure their armed forces and change operational concepts as well, he observed.

27. Mr Tonin touched upon the crucial non-technical and technical challenges of AI adoption in the defence sector. Three key challenges stood out when discussing AI, Mr Tonin argued:

- an investment challenge, since more resources were needed to develop new AI capabilities;
- an innovation challenge, as governments needed to become better and quicker at adopting and integrating AI solutions from the non-defence commercial sectors; and
- a workforce challenge, as countries needed more AI experts and had to retrain those already in the military.

28. Mr Tonin also mentioned the moral, legal, and ethical questions AI raised. He told delegates that he examined the issue of lethal autonomous weapon systems, which would have the capacity to kill without appropriate human supervision. However, he underlined, such weapons did not currently exist, and no state had plans to develop them. Moreover, everyone in the international community agreed humans must retain 'meaningful control' in all autonomous systems. How governments retained 'meaningful control' was, however, a key discussion which had to continue, he argued. Nevertheless, this discussion should not overshadow other moral, legal, and ethical AI questions states already needed to deal with.

29. The STCTTS Rapporteur also discussed some technical challenges. They often concern the data available to AI systems, as the quantity and quality of data were the main 'ingredient' for good AI algorithms. He tackled, in particular, the so-called data diet vulnerability as well as the reliability problem. Mr Tonin also addressed Russian and Chinese ambitions in adopting AI in their armed forces. According to Mr Tonin, the main takeaways of the report were, first, the necessity for Allies to maintain their leadership positions through sustained defence-related AI investments and, second, for the technology gap between Allies to remain small enough to be bridged by interoperability.

30. Opening the discussion, a delegate asked whether it was really true that other international actors were not developing fully autonomous weapons. He also asked how NATO member states should impose restrictions on themselves, for example in terms of industrial policy and ethical and moral issues, when discussing AI developments. Other delegates asked whether countries should look for a small-data solution, since small data sets were increasingly important, and how to collect reliable data for AI applications. The question of data privacy was also addressed by several members. Other members presented opposing opinions on whether AI could really outsmart humans in the future.

31. Rapporteur Tonin said some actors might be willing today to develop fully autonomous weapons, but it was not yet a reality. Furthermore, he stressed the Alliance should highlight that the human had to have meaningful control over any machine. Data privacy was crucial, he observed. Different countries had different regulations and approaches to privacy, he noted, and this was a challenge. He advocated for a high standard of privacy protection. He ended by, once again, underlining the usefulness of AI for the military.

IX. Consideration of the draft Special Report on *NATO Anti-Submarine Warfare: Rebuilding Capability, Preparing for the Future* [089 STC 19 E] by Leona ALLESLEV (Canada), Special Rapporteur, presented by Njall Trausti FRIDBERTSSON (Iceland), STC Vice-Chairperson

32. In presenting the report, **Njall Trausti Fridbertsson** first highlighted the sizeable increase in Russian submarine patrols in NATO areas of operation. More and more Russian submarines were armed with the *Kalibr*, a long-range precision-guided missile, he noted. With this missile, Russia could not only threaten the transatlantic maritime link but also deny access to European shores. The report, he added, also focused on threats to critical undersea communication cables. Other submarine trends should also concern the Alliance, he stressed. China's expanding global forays go hand-in-hand with increasing defence investment, including in submarine modernisation. At the same time, North Korea was seeking to develop submarines armed with sea-launched ballistic missiles with nuclear warheads.

33. Together with the challenges posed by external actors, the Alliance was facing a severe shortfall of anti-submarine warfare capabilities, he stressed. This was both a short- and long-term problem. The number of relevant platforms had fallen, and the current capabilities were rapidly ageing, he argued. On a positive note though, Allies were reacting. In the long term, the seas were becoming louder, given increased maritime traffic, but submarines were harder to detect. Allies should therefore pursue new sensor technologies and the integration of autonomous unmanned vehicles into anti-submarine warfare missions, Mr Fridbertsson added. Finally, the draft report stressed the importance of increased investment in anti-submarine warfare assets.

34. The discussion opened with a request for clarification on the Montreux Convention Regarding the Regime of the Straits by **Taner Yildiz** (TR). He would liaise with Committee staff to put forward his formal proposal. Discussions and questions furthermore revolved around some of the following issues:

- the importance of investments in the right capabilities and their optimisation against new threats;
- the rising threat against undersea cables, which some delegates asked to be fleshed out in the final report;
- detailed discussions on specific anti-submarine warfare capabilities, including unmanned capabilities; and
- clarifications and updates on national capability developments for the fall revision.

35. Mr Fridbertsson thanked members for their interventions. He would pass on the comments and questions to the Rapporteur. Personally, he also underlined the necessity to invest, develop, and improve the Alliance's anti-submarine warfare capabilities.

X. Panel on *China's Science and Technology Challenge* with Helena LEGARDA, Research Associate, Mercator Institute for China Studies (MERICS), Berlin, Germany, and Jan-Peter KLEINHANS, Project Director IoT Security, *Stiftung Neue Verantwortung* (SNV)

36. In her presentation, **Helena Legarda** first explained why the Alliance should pay close attention to Chinese technological developments. In its quest to become a global science and technology superpower, with a military capable of winning wars, China had embarked on an endeavour to surpass Europe and the United States and achieve dominance in the technology sector, she stressed. The one-party system allowed Beijing to adopt a whole-of-government approach to close the technological gap with the West. With a heavily organised top-down process, she explained, China had managed to mobilise the private sector, the government, industry, and the whole society to pursue its goals. Similar efforts had proven difficult for Europe and the United States. For example, Google pulled out of the US Department of Defense's Project Maven, which uses AI to interpret videos and images, due to employee and public concerns over the military uses of the technology. China, she explained, had been incentivising domestic innovation through industrial plans for specific sectors at national and government levels with targets set for localisation, market creation, and productivity.

37. Access to foreign innovation was another path towards technological dominance, she pointed out. Other strategies included talent acquisition; research and development collaboration with international organisations; industrial espionage; exports; and investments in and acquisitions of foreign firms. Ms Legarda concluded her speech by stressing the high speed of Chinese technological progress, thanks to a heavily top-down process. She argued it was up to NATO member states to develop coherent strategies to both promote and protect innovations.

38. **Jan-Peter Kleinhans** underlined the two main reasons justifying the current focus on the 5G networks/Huawei issue. First, the lack of trustworthy information, communication and technology (ICT) in general, and, second, technological dependency of the West on China.

39. Currently, Mr Kleinhans pointed out, it remained impossible to prove the absence of malicious code in technological devices. Standardisation and certification methods could not keep up with the speed at which technology developed. Given this premise, he pointed out, countries needed to trust the company producing the device to fix vulnerabilities as soon as they were discovered. The extent to which a country could trust another one depended on the jurisdiction out of which the supplier operated. With 5G networks, industry and societies would become more vulnerable. Recent recommendations on 5G network risk assessments had called for assessments of the rule of law in countries where potential suppliers are based, he added. Mr Kleinhans underlined how the West remained ill-equipped to develop reasonable ICT security policies. He specified how approaching the 5G issue from the perspective of industrial espionage or sabotage would likely be ineffective.

40. Mr Kleinhans underlined how ICT security policies were fundamental. If countries feared Huawei base stations, they also should fear Alibaba data centres in Frankfurt. However, at what point would this logic become unpractical? With regard to EU efforts on ICT policies, he stressed how technological dependency on China could backfire in future trade disputes and conflicts. The EU should come up with smart and strategic industrial policies to strengthen its ICT sector without disrupting the global ICT supply chain. The focus, he concluded, needed to be on technological dependency, where the EU and the West could produce strategic policies.

41. Questions and comments by delegates included the following:

- How should countries approach the 5G networks/Huawei issue?
- How effective would US President Trump's new China technology policy be and what would its likely long-term consequences be?
- Could China use its market share in rare earth minerals, which are critical for ICT technologies, to coerce other countries?
- How would the Google-Huawei relationship develop in the future?
- How could the EU stimulate innovative growth?
- Could China gain the technological edge over the Alliance?
- Should NATO reposition itself vis-à-vis China?

42. Ms Legarda underlined how the case of Huawei was very specific. The Communist Party of China stood behind the company, as 98% of the company was controlled by the Party. She stressed how the party was above the law and how every Chinese company and individual was required to collaborate with authorities when the party raised national security concerns. What the party considered national security was a very broad concept, she argued. Huawei could act as a private company for now, she underlined, but when asked it would respond to the Party's demands. Current US policy, she went on, made clear how China was still dependent on the United States, as it had had negative effects on the Chinese economy. While the policy put critical issues on the agenda, it would not change China's course over the long term. China would not give up its technology policies because of US policy. The Chinese priority was to maintain the status quo. China was prepared to suffer the economic consequences to achieve its goal. She did not think US-EU talks with China could improve the situation which had become very ideological.

43. Regarding China's threat to rare earth mineral supplies, Mr Kleinhans said this particular issue remained a niche issue. China remained dependent on the United States for microchips and had overestimated this specific pressure point.

44. During the discussion, Ms Legarda pointed out that Huawei had already invested in creating its own operating system, as the company had been foreseen a risk to be shut out of Android and iOS at some point. However, underlined Mr Kleinhans, Huawei was still far behind Apple, Google, and Microsoft. China, he went on, understood the need to become more independent and, in retaliation, had published its own list of untrustworthy 'Western' companies. Ms Legarda also warned that some efforts against Chinese companies might hurt both China and the 'West', as supply chains are heavily integrated. Regarding the future of Chinese innovation, Ms Legarda observed that innovation was certainly possible, but the undemocratic and closed Chinese state was a clear obstacle.

45. Mr Kleinhans argued the EU lacked a strategic industrial policy. Since top-down regulation would not work for the EU and subsidies would not be enough, the EU needed to understand its place in the ICT supply chain. It needed to produce policies to fund and support small- and medium-sized companies since they had become easy targets for Chinese acquisition.

46. On NATO repositioning, Ms Legarda stressed the need not to lose sight of conventional threats while looking at China as a global player. China was already in Europe, through military exercises with Russia and navigation operations in the Mediterranean and Baltic Seas. A conventional presence in the Pacific was not necessary, however, she concluded. From a technological perspective, Mr Kleinhans added, countries and their armies and societies depended more and more on technology and the use of commercially operated mobile networks. NATO should focus on the impact of ICT on international security, and like-minded Allies should build more resilient security systems, he concluded.

XI. Summary of the future activities of the Science and Technology Committee and of the Sub-Committee on Technology Trends and Security (STCTTS)

47. The Chairperson proceeded by outlining the recent and future activities of the STC. Members were briefed on how the STC delegation on its recent Singapore visit learned how disruptive inventions and innovations were impacting the defence and security, but also the civilian sector.

48. With regard to future visits, the STCTTS would visit London and South England from 17 to 20 June. This visit would focus on defence science and technology, cybersecurity and defence, AI, machine learning and big data, anti-submarine warfare, and maritime defence and security. Finally, the third visit would possibly take place in Norfolk, Virginia, and Washington, D.C. at the end of October/early November. The NATO Allied Command Transformation, the NATO new Joint Force Command-Norfolk, and the US Second Fleet would likely be part of the visit. This was a change in the STC programme of activities, as planned participation in an anti-submarine warfare exercise off the coast of Canada was no longer feasible, due to logistical reasons.

XII. Any other business

49. The 2019 Spring Session marked the last full Committee meeting of STC Chairperson Maria Martens, as she had decided not to stand for another election in the Dutch Senate. STC Vice-Chairperson **Bruno Jorge Vitorino** (PT) took the opportunity and honoured her career. On behalf of the Committee, Mr Vitorino thanked her for her excellent chairing of the STC and wished her luck in her future endeavours.

XIII. Date and place of next meeting

50. Ms Martens reminded members that the next Committee meeting would take place at the Annual Session in London in October.

XIV. Closing remarks

51. Concluding the meeting, the Chairperson thanked the members and speakers for their constructive contributions and the Slovak Delegation and its staff for a well-organised session.

52. She thanked the interpreters, the Committee Director, Committee Coordinator, and the research assistants taking notes. Finally, she adjourned the meeting of the STC at the 2019 Spring Session.