Chair report on Cyber Champions Summit 2023[1]

National cyber coordinators from NATO countries and closest partners from Asia-Pacific region, met in Vilnius to discuss pressing cyber security challenges, to coordinate a response measures, and to lay the foundation for a more structured cyber dialogue between NATO and Asia-pacific countries. This meeting also served as a platform for the development of cyber related deliverables for the NATO summit in Vilnius.

According to Lithuania's point of view, different state and non-state actors, including Russia, Belarus, North Korea, Iran, China, and others are using cyberspace increasingly as a platform from which to target critical infrastructure, undermine democracies and undercut fair competition in global arena. Cyber domain has played and continues to play a very important role in Russia's war against Ukraine. Also, cyber domain is heavily used by other malign cyber actors to conduct economic espionage and get access to sensitive information.

Participating countries discussed how lessons identified from the war in Ukraine and behaviour of other malign cyber actors could be turned into lessons learned by the global like-minded community. The discussion among NATO members highlighted importance of further strengthening NATO cyber resilience and defence, with a particular focus on virtual cyber response capabilities, and enhancing NATO's support to Ukraine.

Our meeting benefited to defining priority areas for closer NATO and Asia-Pacific cooperation on cyber, including enhanced information sharing, policy coordination and exercises. A need to launch a more structured NATO cyber dialogues with AP4 countries has been underlined, this issue could be addressed in the upcoming NATO summit in Vilnius. In addition, participation in joint initiatives such as Counter Ransomware Initiative or Regional Cyber Defence Centre in Kaunas are good platforms to accelerate information sharing and coordinated response efforts in countering cyber threats.

The meeting was followed by in-depth discussions about the protection of critical infrastructure and possibility to enhance cooperation. Today's digital landscape is closely interconnected and cyber security threats pose significant risks to critical infrastructure. On top of that, Emerging Disruptive Technologies (EDTs) introduce new risks and vulnerabilities. Governments must consider the potential impacts of EDTs on supply chain security and cyber security measures. Strong supply chains are the backbone of a resilient economy, they rely on well-secured critical infrastructure. Failure to do so could have serious implications to the well-being of our societies not only at the national, but also at the global level.

Cyber Champions Summit from now on is a like-minded platform among European, Asia-Pacific and North American partners to discuss and guide our joint efforts in strengthening cyber resilience and defence. Australia with Lithuania will consider next steps for maintaining the momentum established from this year's Cyber Champions Summit. We will continue to work together to ensure continuous discussions and preparation for the next Summit to deepen the expertise and cover broad spectrum of cyber challenges.

[1] Report below presents the view of a Cyber Champions Summit Chair – Deputy Minister of National Defence of the Republic of Lithuania Greta Monika Tučkutė