

Developing Practical Cooperation through Science

Finland has been actively engaged within the framework of the NATO Science for Peace and Security (SPS) Programme since 1994.

The NATO SPS Programme enables close collaboration on issues of common interest to enhance the security of NATO and Partner nations by facilitating international efforts to meet emerging security challenges, supporting NATO-led operations and missions, and advancing early warning and forecasting for the prevention of disasters and crises.

The current SPS Key Priorities include:

- *Counter-Terrorism;*
- *Energy Security;*
- *Cyber Defence;*
- *Defence against CBRN Agents;*
- *Environmental Security;*
- *Security-related Advanced Technology;*
- *Border and Port Security;*
- *Human and Social Aspects of Security.*

Additionally, the SPS Programme helps to promote *regional security* through scientific cooperation among Partners. The Programme also helps to *prepare* interested eligible nations for NATO membership. SPS activities often have a high *public diplomacy* value.

FINLAND

The SPS Programme strongly welcomes collaboration with Finland in future activities. At present, Finland is leading four ongoing activities under the framework of the SPS Programme. The primary areas of cooperation with Finland are: **Counter-Terrorism, Cyber Defence, Advanced Technology** and **CBRN Defence**. Below are some examples of ongoing and completed projects led by Finnish scientists and experts.

Cooperative Activities

INTELLIGENT AND RESILIENT CYBER DEFENCE IN SUPPLY CHAINS AND LOGISTICS

The overall objective of this project is to develop an efficient cyber defence for intelligent systems, such as modern automated supply chains, military supply chains, and logistics systems of a 4th generation. The scope of the project is to train the Artificial Intelligence (AI)-systems to recognise a potential cyber-attack, including its “*symptoms*” and structurally respond to it. The project will also model feasible data attack scenarios and propose an architecture to increase system immunity against adversary data flows. It will increase the potential to share and further develop the expertise essential for the creation and implementation of advanced concepts and tools for adaptive cyber defence and intrusion prevention in AI-based systems. *This project is led by scientists and experts from Finland and Bulgaria, and also involves experts from France and Ukraine.* [ref. G5511].

INTEGRATED SYSTEM FOR THREATS EARLY DETECTION (INSTEAD)

INSTEAD is the third Multi-Year Project (MYP) related to DEXTER - a follow-on of the STANDEX programme - to detect explosives and firearms. The main objective of this ongoing project is to deliver a system for the centralized management of sensors deployed in a specific location to improve the detection capabilities of person-borne explosives in moving crowds. INSTEAD will interface sensors developed in its sister projects, and a video system to enhance capabilities to raise the alarm on suspects in emergency and intervention protocols. *This project is led by Finland and Italy, and also involves experts from The Netherlands.* [ref. G5605].

PORTABLE LOW-COST RAMAN PROBE FOR CHEMICAL CONTAMINANT IDENTIFICATION (RAPID)

This MYP aimed to develop and demonstrate a reliable, low-cost, label-free Surface Enhanced Raman Scattering (SERS) sensor probe, which will be employed to detect major contaminants in water-like Polycyclic Aromatic Hydrocarbons, Ammonia, Nitrates, Herbicides and Pesticides. The technology presented a breakthrough in applying photonic sensing to chemical and biological defence, and will provide a much-needed cost-effective technology for the quick detection of CBRN threats on the field with portable devices. This is a crucial step forward considering that previous methods for analysing water require hours. *This project, completed in 2019, was led by experts from Finland, Italy, and Spain.* [ref. G5250].

DEVELOPING A MULTINATIONAL TELEMEDICINE SYSTEM FOR EMERGENCY SITUATIONS

The aim of this flagship MYP was to develop a multinational telemedicine system to improve access to health services and increase survival rates in emergency situations, particularly in remote areas. Through the use of modern communication technologies, an international network of medical specialists will be able to assess patients, determine diagnoses and provide real-time recommendations. The technology was successfully live-tested during field exercises in Ukraine, Montenegro and Bosnia and Herzegovina. *This project was led by Finland and Romania, and also involved experts from the United States, the Republic of Moldova and Ukraine.* [ref. G4748].



Live testing of the telemedicine system during the Ukraine 2015 field exercise attended by Secretary General Stoltenberg and President Poroshenko.

CYBER DEFENCE IN INDUSTRY 4.0 SYSTEMS

The majority of advanced industry 4.0 systems and related logistics and infrastructures (including those employed in the military and defence sector) are vulnerable to cyber-attacks. Consequences of such attacks could be severe. For example, entire industrial, logistics and transport sectors could be immobilized, having a substantial impact on national security. Therefore, the systems must be well protected from intrusions. To ensure their protection, adaptive cyber defence capabilities must be developed and effectively implemented. These include the implementation of advanced technologies without human intervention, as well as improvement and reconfiguration of the corresponding IT infrastructures. In October 2017, an Advanced Research Workshop (ARW) was held in order to establish strategies, concepts and tools for the creation and implementation of cyber systems and 4G cyber platforms capable of:

- providing enhanced cyber defence and interoperability,
- smart intrusion prevention,
- adaptive cyber defence,
- smart recovering of the system states,
- smart monitoring, control and management of industry 4.0 systems and related logistics and IT infrastructure.

The workshop also established a network of civilian and military experts from Allied and partner countries, creating a forum to share their respective expertise in the field. *This workshop was led by experts from Finland and Bulgaria.* [ref. G5172].



The NATO Science for Peace and Security Programme

www.nato.int/science