The NATO Science for Peace and Security Programme

CountryFlyer 2022

August

QATAR

Developing Practical Cooperation through Science

Qatar has been actively engaged with NATO since the creation of the Istanbul Cooperation Initiative (ICI), launched at the Istanbul Summit in 2004.

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.

Qatar is engaged with the Science for Peace and Security (SPS) Programme and NATO through the Istanbul Cooperation Initiative (ICI) partnership framework. Leading areas of cooperation include **Cyber Defence** and **Security-related Advanced Technology.** The SPS Programme is open to new activities with Qatar, in line with the Allies' political guidance in the form of the 2012 Key Priorities for the SPS Programme.

Cooperative Activities

DEVELOPING PHYSICAL-LAYER SECURITY SCHEMES FOR INTERNET OF THINGS NETWORKS

Internet of Things (IoT) is the global concept of interrelated computing devices, digital machines and sensors capable of communicating and transferring data over a network. Currently, billions of devices around the world are connected to the internet, all collecting and sharing data. Thanks to the increase of low-cost computer chips and the ubiquity of wireless networks, in the future it will be possible to connect any electronic device to IoT, allowing them to communicate in real-time without involving humans. Distributed nodes in IoT networks could be vulnerable entry points for overall security. This project, therefore, aims to develop lightweight security mechanisms tailored for IoT networks based on physical-layer security approaches. The project will address data confidentiality in IoT networks; propose novel authentication protocols; assess the trade-off between security and energy efficiency in proposed and conventional methods; propose security-based detection schemes for malicious and malfunction nodes; and evaluate the proposed methods through computer simulations and hardware implementation. *This project is led by Qatar, Portugal and Jordan.* [ref. G5797].

PROTECTION OF CYBER-PHYSICAL SYSTEMS AGAINST MALICIOUS ATTACKS

Cyber-physical systems infrastructure requires the development of novel and proactive security technologies now more than ever. In many Allied and partner nations, these systems are being targeted for attacks and intrusions by intelligent adversaries. This Multi-Year Project (MYP) aimed to develop an innovative approach to the research, evaluation, design and development of attack-monitoring and attack-resilient control recovery methodologies and toolkits to ensure and improve the sustainability, survivability, resiliency, and availability of cyber-physical systems. *This project was completed in 2022, and was led by Qatar, Canada, Japan and Australia.* [ref. G5479].

SEASEC: DRONETS FOR MARITIME BORDER AND PORT SECURITY

This MYP was launched in 2021 and addresses the challenge of ensuring proper situational awareness at sea by enhancing traditional border and port surveillance systems with quickly deployable squads of Unmanned Aircraft Systems (UAS) or drones (DroNet) that autonomously cooperate to deliver relevant, complete and up-to-date information. UAS are usually controlled remotely by a human operator or can fly autonomously by on-board computers. They can be equipped with several types of sensors, including video and/or thermal cameras, to detect and report alerts to a central system. The project will enhance the state-of-the-art technology for border and port security by providing new techniques that will contribute to the realization of an accurate, complete, and efficient monitoring system. These techniques will provide Maritime Domain Awareness (MDA), defined as the effective understanding of any activity associated with the maritime environment that could affect the economy, environment or safety. *This project is led by scientists from Qatar and Italy.* [ref. G5828].

WOMEN IN CYBER SECURITY

This Advanced Research Workshop (ARW) took place in Doha, Qatar, in October 2019. The "Women in Cyber Security" workshop is an initiative by the KINDI Center for Computing Research at Qatar University that encourages and empowers women in the field of cyber security. The goal of the event was to highlight female role models in cyber security who shared inspiring success stories of knowledge development and achievement with the participants. The event brought together women from NATO and partner countries to share knowledge, enhance their networking abilities, explore opportunities for collaboration, and get to know local female leaders in cyber security. *This workshop was led by experts from Qatar and France.* [ref. G5666].

THE ISTANBUL COOPERATION INITIATIVE

The Istanbul Cooperation Initiative (ICI) focuses on practical cooperation in areas where NATO can add value, notably in the security field. Initially, six countries of the Gulf Cooperation Council were invited to participate. To date, four of these – Bahrain, Qatar, Kuwait, and the United Arab Emirates – have joined. Saudi Arabia and Oman have also shown an interest in the Initiative. Based on the principle of inclusiveness, the Initiative is however open to all interested countries of the broader Middle East region who subscribe to its aims and content, including the fight against terrorism and the proliferation of weapons of mass destruction.

The ICI is a 'two-way' partnership, in which NATO seeks Partners' contribution for its success, through a regular consultation process, where special emphasis is placed on practical cooperation. The SPS Programme is an excellent basis for such practical and concrete partnership activities.