Emerging Security Challenges Division

Science for Peace and Security Programme

Call for Proposals on:

Cyber Defence

Background

Cyber threats and attacks are becoming more frequent, sophisticated and damaging. The Alliance of today faces an evolving and complex threat environment previously unseen in this domain of operations. Both state and non-state actors have the ability to use cyber-attacks which could be as harmful to modern societies as a conventional attack as well as increasingly incorporating cyber-attacks within hybrid warfare. Further enhancing partnerships with other international organisations and partner nations, likewise with industry and academia, plays a key role in effectively addressing the challenges of cyber defence. NATO's Science for Peace and Security (SPS) Programme is issuing a Call for Proposals, in line with its key cyber defence priorities, to target scientific and technological advancements in the field of cyber defence. These key priorities are as follows:

i. Critical infrastructure protection, including sharing of best practices, capacity building and policies;
ii. Support in developing cyber defence capabilities, including new technologies and support to the construction of information technology infrastructure;
iii. Cyber defence situation awareness.

Scope

The scope of this call solicits proposals in the following areas:

- *Operational Cyber Security* – Support for Computer Security Incident Response Teams (CSIRTS)
  - *Incident Management and Response* – solutions which include typology, service catalogue, models, performance evaluation, information sharing, wargaming, exercises, legal frameworks.
- *Cyber Security Technology* – Solutions for defending against cyber-terrorism, cyber-physical attacks, zero-day attacks, ransomware, Distributed Denial of Service (DDoS), malware and botnets.
  - *Security of Cyber-Physical Systems* – defending cyber-physical systems, such as VANET/IoV, SUAVs, mobile tactical networks and airborne/maritime units, against cyber-attacks that cross over to the physical domain (malware, network protocol attacks, security misconfiguration, code/data injection etc.) as well as physical attacks that cross over to the cyber domain (covert/confusing signal emission, physical bit injections to memory/processor bus, memory bit flipping etc.).
  - *Software Security Assurance* – obtaining measurable/predictable software security, including security metrics and evaluation methods, vulnerability detection and prediction, efficient and scalable formal/AI based methods, automated/real time application security risk assessment.
  - *Crypto Ransomware Mitigation Techniques* – efficient and robust mitigation solutions for crypto ransomware families.

- *Distributed Trust Mechanisms* – solutions based on distributed cryptography are needed to avoid single-point-of-failure for various scenarios ranging from secure messaging to secure cloud storage and providing audit compliance.
- *Secure Hardware Platforms* – hardware based solutions to provide key storage and support data protection, by leveraging Trusted Platform Modules (ISO/IEC 11889) or alternative approaches.

- *Quantum Safe Solutions* - design and implementation of cryptographic solutions in settings where an adversary may have access to large-scale quantum computing resources.
  - *Secure/Verifiable Computation* – practical quantum-safe solutions for secure and verifiable distributed and outsourced computation, possibly supported by Fully Homomorphic Encryption (FHE).
  - *Secure Group Communication* – quantum-safe solutions for group communication with a focus on, but not limited to, authenticated key establishment, key management, dynamic properties and hierarchical structures.
- *Cyber Security Strategies and Policies.*

Funding mechanisms

The SPS Programme supports collaboration through three established grant mechanisms: multi-year research projects (MYP), workshops (Advanced Research Workshop), and training courses (Advanced Studies Institutes/Advanced Training Courses). Interested applicants should develop proposals for activities that fit within one of these formats. Application forms for SPS workshops, training courses, and multi-year projects can be downloaded from: ***www.nato.int/science***.

Programme Requirements

As one of the principal goals of the Science for Peace and Security Programme is to promote cooperation between NATO countries and NATO partner countries, only applications from researchers in those countries (see below) can be accepted.
Applications should be submitted to *sps.applications@hq.nato.int* and all relevant enquiries shoul be submitted to *sps.info@hq.nato.int*

The deadline for applications is 31 October 2017.

NATO Countries

Albania, Belgium, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Italy, Latvia, Lithuania, Luxembourg, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Turkey, United Kingdom, United States.

Eligible NATO Partner Countries

Afghanistan, Algeria, Armenia, Australia, Austria, Azerbaijan, Bahrain, Belarus, Bosnia and Herzegovina, Columbia, Egypt, Finland, Georgia, Iraq, Ireland, Israel, Japan, Jordan, Kazakhstan, Kuwait, Kyrgyz Republic, Malta, Mauritania, Moldova, Mongolia, Morocco, New Zealand, Pakistan, Qatar, Republic of Korea, Serbia, Sweden, Switzerland, Tajikistan, the former Yugoslav Republic of Macedonia†, Tunisia, Turkmenistan, Ukraine, United Arab Emirates, Uzbekistan.

†Turkey recognises the Republic of Macedonia with its constitutional name.