July 2016

# NATO Cyber Defence

Cyber threats and attacks are becoming more common, sophisticated and damaging. The Alliance is faced with an evolving complex threat environment. State and non-state actors can use cyber attacks in the context of military operations. NATO and its Allies rely on strong and resilient cyber defences to fulfil the Alliance's core tasks of collective defence, crisis management and cooperative security. NATO needs to be prepared to defend its networks and operations against the growing sophistication of the cyber threats and attacks it faces.

## NATO Policy on Cyber Defence

To keep pace with the rapidly changing threat landscape, NATO adopted an enhanced policy and action plan on cyber defence, endorsed by Allies at the Wales Summit in September 2014. The policy establishes that cyber defence is part of the Alliance's core task of collective defence, confirms that international law applies in cyberspace and intensifies NATO's cooperation with industry. The top priority is the protection of the communications and information systems owned and operated by the Alliance.

The policy also provides for streamlined cyber defence governance, procedures for assistance to Allied countries in response to cyber attacks, and the integration of cyber defence into operational planning, including civil emergency planning. Further, the policy defines ways to take awareness, education, training and exercise activities forward, and encourages further progress in various cooperation initiatives, including those with partner countries and international organisations. It also foresees boosting NATO's cooperation with industry, including on information sharing, the exchange of best practices and the exploration of innovative technologies to enhance cyber defence. Allies have also committed to enhancing information sharing and mutual assistance in preventing, mitigating and recovering from cyber attacks.

At the Warsaw Summit in July, NATO Heads of State and Government are expected to recognise cyberspace as an operational domain, in addition to air, land and sea. Treating cyberspace as an operational domain will enable the Alliance to better protect its missions and operations, with more focus on training and military planning. It will also give NATO a better framework to manage resources, skills, capabilities and coordinate decisions. This will not change NATO's mission or mandate, which is defensive. As in all operational domains, NATO's actions are defensive, proportionate and in line with the international law.

The Alliance also welcomes efforts undertaken in other international fora to develop norms of responsible state behaviour and confidence-building measures to foster a more transparent and stable cyberspace for the international community.

## Developing NATO cyber defence capability and capacity

The NATO Computer Incident Response Capability (NCIRC) protects NATO's own networks by providing centralised and round-the-clock cyber defence support to various NATO sites. It handles and reports incidents, and disseminates important incident-related information to system/security management and users. NCIRC also maintains Rapid Reaction Teams, which can be deployed to support the protection of NATO or Allied networks.

NATO helps Allies in their efforts to protect their own critical networks and infrastructures by sharing information and best practices. A Memorandum of Understanding on Cyber Defence between NATO and each of the 28 Allied cyber defence authorities sets out arrangements for the exchange of a variety of cyber defence related information and assistance to improve cyber incident prevention, resilience and response capabilities.

To facilitate an Alliance-wide and common approach to cyber defence capability development, NATO also develops targets for Allied countries' implementation of national cyber defence capabilities through the NATO Defence Planning Process. In 2017, further cyber defence capability targets will be agreed.

NATO conducts regular exercises, such as the annual Cyber Coalition Exercise, and aims to integrate cyber defence elements and considerations into the entire range of Alliance exercises. NATO is also enhancing its capabilities for cyber education, training and exercises, including the NATO Cyber Range.

The **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defence education, consultation, lessons learned, research and development. Although it is not part of the NATO Command Structure, the Centre offers recognised expertise and experience on cyber defence.

The **NATO Communications and Information Systems School** in Latina, Italy provides training to personnel from Allied (as well as non-NATO) nations relating to the operation and maintenance of some NATO communication and information systems. The school will soon relocate to Oeiras in Portugal, where it will provide greater emphasis on cyber defence training and education.

The **NATO School** in Oberammergau, Germany also conducts cyber defence-related education and training to support Alliance operations, strategy, policy, doctrine and procedures. The **NATO Defense College** in Rome, Italy fosters strategic thinking on political-military matters, including on cyber defence issues.

## Cooperating with partners

As cyber threats defy state borders and organisational boundaries, NATO engages with relevant countries, organisations and private sector to enhance international security.

NATO works with, among others, the European Union (EU), the United Nations (UN), the Council of Europe and the Organization for Security and Cooperation in Europe (OSCE). In February 2016, NATO and the EU concluded a Technical Arrangement on Cyber Defence to help both organisations better prevent and respond to cyber attacks. This Technical Arrangement provides a framework for exchanging information and the sharing of best practices between emergency response teams.

## Cooperating with industry

The private sector is a key player in cyberspace. Technological innovations and expertise from the private sector are crucial to enable NATO and Allied countries to mount an effective cyber defence. Through the NATO Industry Cyber Partnership (NICP), NATO and its Allies are working to reinforce their relationships with industry. This partnership relies on existing structures and will include NATO entities, national Computer Emergency Response Teams (CERTs) and NATO member countries' industry representatives. Information sharing activities and exercises, education and training are just a few examples of areas in which NATO and industry have been working together.

**Public Diplomacy Division (PDD) – Press & Media Section**
**Tel.: +32(0)2 707 5041**
**E-mail: moc@hq.nato.int**
**Follow us @NATOpress**

**www.nato.int**

1090-16 NATO Graphics & Printing