May 2017

# NATO Cyber Defence

Cyber threats are becoming more common, sophisticated and damaging. Recent high-level cyber-attacks against NATO Allies demonstrate that cyber defence and resilience should be a top priority.

## NATO's approach to cyber defence

At the 2014 NATO Summit in Wales, Allies recognised that international law applies in cyberspace, and that the impact of cyber-attacks could be as harmful to our societies as a conventional attack. As a result, cyber defence was recognised a part of NATO's core task of collective defence.

At the Warsaw Summit in 2016, Allies took additional steps by recognising cyberspace as a domain of operations – just like air, land and sea. In concrete terms, this enables NATO's military structures to devote specific attention to protecting missions and operations from cyber threats.

The recognition of cyberspace as a domain does not change NATO's mandate. As in all operational domains, NATO's actions are defensive, proportionate and in line with international law.

At the Warsaw Summit, Allies also adopted the Cyber Defence Pledge to strengthen and enhance the cyber defences of national networks and infrastructures. Each Ally is responsible for its own cyber defences, but NATO helps Allies in many ways. The continuous adaptation of NATO's cyber defence capabilities reinforces the cyber defences and overall resilience of the Alliance.

## Cyber-attacks against NATO

NATO has been increasingly targeted with cyber-attacks over the past decade. The majority of targeted attacks against NATO networks originate from state actors.

Suspicious events are detected every day. Most of these are dealt with automatically. Some require analysis and response by NATO's cyber defence experts. In 2016 NATO experienced an average of 500 incidents per month – an increase of roughly 60% over 2015. This reflects an increase in the number of cyber-attacks, but also a wider network coverage and protection.

## NATO's cyber defence capabilities

The **NATO Computer Incident Response Capability** (NCIRC) based in SHAPE, Mons, protects NATO's own networks through round-the-clock cyber defence support. Its team of 200 experts handles incidents and provides NATO and Allies with up-to-date analysis of the cyber challenges we face.

NATO helps Allies to boost their cyber defences by:

- Sharing real-time information about threats through a dedicated malware information sharing platform, as well as best practices on handling cyber threats;
- Maintaining rapid-reaction cyber defence teams that can be sent to help Allies in handling cyber challenges;
- Developing targets for Allies to facilitate a common approach to their cyber defence capabilities;
- Investing in education, training and exercises.

Several bodies associated with NATO are also helping the Alliance to improve cyber defences.

The **NATO Cyber Range** in Tartu, Estonia, is used by cyber experts to develop their capabilities through realistic exercises. The Cyber Range hosts NATO's flagship annual cyber defence exercise "Cyber Coalition".

The **NATO Cooperative Cyber Defence Centre of Excellence** in Tallinn, Estonia is a NATO-accredited research and training facility dealing with cyber defence education, research and development. The Centre offers recognised expertise 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 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-related education and training to support Alliance operations, strategy, policy, doctrine and procedures.

The **NATO Defence College** in Rome, Italy fosters strategic thinking on political-military matters, including on cyber defence issues.

## Cooperation with partners

Partnerships play a key role in effectively addressing cyber challenges. NATO engages with a wide range of partners – including international organisations, industry and academia.

Cyber defence is one of the areas of strengthened cooperation between NATO and the European Union, as part of the two organisations' increasingly coordinated efforts to counter hybrid threats. NATO and the EU are working more closely in this area than ever – including sharing information between cyber crisis response teams and exchanging best practices.

NATO is also helping partner countries tackle cyber challenges. One of the NATO Trust Funds in support to Ukraine is focused on cyber defence.

## Cooperation with industry

The private sector is a key player in cyberspace and its expertise is crucial for cyber defence.

NATO is strengthening its relationship with industry through the NATO Industry Cyber Partnership, which supports NATO's efforts to protect our networks, increase resilience to cyber threats and help Allies develop their cyber capabilities.

Information sharing, exercises, training and education are just a few examples of areas where NATO and industry are working together.

**Public Diplomacy Division (PDD) – Press & Media Section**
**Tel.: +32(0)2 707 9867**
**E-mail: moc@hq.nato.int**
**Follow us @NATOpress**

**www.nato.int**

0960-17 NATO Graphics & Printing