NATO OTAN North Atlantic Treaty Organization

www.nato.int/factsheets Factsheet

August 2020

NATO Cyber Defence

Cyber threats to the security of the Alliance are becoming more frequent, complex, destructive, and coercive. Enhancing the cyber defences and resilience of both NATO as an organisation and its 30 Allies is a top priority.

NATO's approach to cyber defence

Allies recognise that a cyber-attack could be as harmful to our societies as a conventional attack. As a result, cyber defence is part of NATO's core task of collective defence.

NATO recognised cyberspace as a domain of operations in 2016 alongside the traditional domains of air, land and sea. This enables NATO's military commanders to better protect missions and operations from cyber threats, including by drawing on Allies' national cyber capabilities. Allies keep full ownership of these capabilities – just as Allies own tanks, ships and aircraft. As in all other domains, in cyberspace NATO's actions are defensive, proportionate and in line with international law. Allies agree that we all stand to benefit from a rules-based, predictable, open, free, and secure cyberspace.

While each Ally is responsible for its own cyber defences, NATO serves as a platform for Allies to consult on cyber defence issues, share information on cyber threats, exchange best practice, and coordinate activities. NATO supports its members in boosting cyber defences, for example by:

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

In line with their national responsibilities and competences, Allies are committed to protecting their critical infrastructure, building resilience and bolstering cyber defences, including through full implementation of NATO's Cyber Defence Pledge.

Malicious cyber activities against NATO

NATO's IT infrastructure covers over 60 different locations – from the political headquarters in Brussels, through military commands to the sites of NATO operations. More than 100,000 people rely upon NATO networks. These have been increasingly targeted with malicious cyber activities over the past decade.

NATO cyber defence systems register suspicious events each day: from low-level attempts to technologically sophisticated attacks against NATO networks. The majority are detected and dealt with automatically. Some require analysis and response by our experts. A 200-strong cyber team defends NATO's networks around the clock. It prevents intrusions, detects, analyses and shares information on malware, prevents data loss, and conducts computer forensics, vulnerability assessments and post-incident assessments.

NATO's cyber defence structures

The **NATO Computer Incident Response Capability** (NCIRC) based in SHAPE, Mons, protects NATO's own networks through round-the-clock cyber defence support. Its experts handles incidents and provides NATO and Allies with up-to-date analysis of the cyber challenges we face. The NCIRC is part of the NATO Communications and Information Agency, which supports NATO operations, connects NATO's information and communication systems, and defends NATO's networks.

NATO has established a **Cyberspace Operations Centre** in Mons, Belgium. The Centre supports military commanders with situational awareness to inform the Alliance's operations and missions. The centre will also coordinate NATO's operational activity in cyberspace, ensuring freedom to act in this domain and making operations more resilient to cyber threats.

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 provides valuable expertise on cyber defence, and organises cyber exercises involving both NATO Allies and partners.

The **NATO School** in Oberammergau, Germany conducts cyber defence-related education to support Alliance operations, strategy, policy, doctrine and procedures. The **NATO Communications and Information Academy**, which has been established in Oeiras, Portugal, provides training for NATO's cyber defence workforce. Finally, 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 share information between cyber incident response teams and exchange best practices.

NATO is also helping partner countries tackle cyber defence challenges. For example, NATO supports training activities on cyber defence through the Science for Peace and Security (SPS) Programme as well as national cyber defence capacities through the Defence and Capacity Building assistance framework.

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

0810-20 NATO Graphics & Printing

Printed on 100% recycled paper