NATO OTAN
North Atlantic Treaty Organization

www.nato.int/factsheets Factsheet

February 2019

NATO Cyber Defence

Cyber threats continue to evolve. Recent high-level cyber-attacks against NATO Allies demonstrate that bolstering our cyber defences and resilience should be a top priority.

NATO's approach to cyber defence

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

NATO declared cyberspace as a domain of operations – just like air, land and sea - at the Warsaw Summit in 2016. This enables NATO's military commanders to better protect missions and operations from cyber threats.

Allies are also strengthening the cyber defences of their national networks and infrastructures through initiatives such as the Cyber Defence Pledge, adopted in 2016. This is central to enhancing cyber resilience.

While each Ally is responsible for its own cyber defences, NATO supports its members in boosting these defences, for example by:

- Sharing real-time information about threats through a dedicated malware information sharing platform, as well as exchanging best practices on handling 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.

NATO has also put in place policies that will allow it to draw on Allies' national cyber capabilities in its operations and missions, in line with its defensive mandate and subject to political control. Several Allies have offered their sovereign cyber effects for the benefit of NATO operations and missions. 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.

Cyber-attacks 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 cyber-attacks 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 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 team of 200 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.

As part of the reinforcement of its cyber defences, NATO is setting up a new **Cyber Operations Centre** in Mons, Belgium. The Centre will be fully operational in 2023. It will support our military commanders with situational awareness to inform our operations and missions, and strengthen NATO's cyber defences. The centre will also coordinate NATO's operational activity in cyberspace, ensuring our freedom to act in this domain and making our operations more resilient to cyber-attacks.

NATO as an organisation has no plans to develop its own offensive cyber capabilities. At the same time, Allies can volunteer their **sovereign cyber effects** for NATO operations and missions. Allies will retain control of their national cyber capabilities at all times when they are used in a NATO context. Several Allies have already offered their national cyber effects to NATO. This ensures NATO's defences continue to evolve at a pace with the fast-moving cyber threats.

The **NATO Cyber Range** in Estonia, is a platform for NATO exercises and training in Estonia. It is operated by the Estonian Defence Forces. The Cyber Range facilitates 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 provides valuable expertise on cyber defence, and organises cyber exercises involving both NATO Allies and partners.

The **NATO School** in Oberammergau, Germany conducts cyber-related education to support Alliance operations, strategy, policy, doctrine and procedures. Training for NATO's cyber workforces will also be provided by the **NATO Communications and Information Academy**, which is currently being built in Oeiras, Portugal. 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 challenges. For example, one of the NATO Trust Funds in support to Ukraine is focused on cyber defence. Cyber defence is also an area where NATO supports Jordan, as part of our Defence and Capacity-Building assistance.

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 5041
E-mail: moc@hq.nato.int
Follow us @NATOpress
www.nato.int

0177-19 NATO Graphics & Printing

Printed on 100% recycled paper