February 2018

NATO Cyber Defence

Cyber threats continue to evolve. 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 recognised cyberspace as a domain of operations – just like air, land and sea. This enables NATO's military commanders to better protect 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 the cyber defences of national networks and infrastructures. Each Ally is responsible for its own cyber defences, but NATO helps Allies in many ways.

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. Throughout 2017, NATO cyber experts noted an evolution in cyber attacks, and increasing targeting of softer systems, such as personal devices and networks related to NATO but not covered by its protection.

NATO's cyber defence capabilities

As part of the reinforcement of its cyber defences, in 2017 NATO Allies agreed to create a new **Cyber Operations Centre**. Work on its set-up is ongoing.

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, such as Cyber Coalition, one of the largest cyber defence exercises in the world.

Several bodies are also helping the Alliance and individual nations to improve cyber defences.

The NATO Communications and Information Agency, with headquarters in Brussels and Mons (Belgium) and The Hague (the Netherlands), supports NATO operations, connects NATO's information and communication systems, and defends NATO's networks.

The **NATO Cyber Range** in Tartu, Estonia, is used by cyber experts to develop their capabilities through realistic exercises. 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 offers recognised expertise on cyber defence.

The NATO Communications and Information Academy is being built in Oeiras, Portugal. Once up and running in 2019, the Academy will train thousands of civilian and military personnel a year, and make a major contribution to NATO's cyber defences. 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 share information between cyber crisis response teams and exchange 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 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

0233-18 NATO Graphics & Printing