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

Cyber defence is part of NATO's core task of collective defence. The Alliance considers cyber space an operational domain in which it must defend itself as effectively as it does in the air, on land and at sea. This does not change NATO's mandate - as in all operational domains, NATO's actions are defensive, proportionate and in line with international law.

In cyber space, NATO's priority is the protection of its communication and information systems. Allies are responsible for their own cyber defences, but NATO helps them in many ways.

NATO's policy on cyber defence was adopted at the Wales Summit in 2014. And at the Warsaw Summit in 2016, Allies committed through a Cyber Defence Pledge to strengthen and enhance the cyber defences of national networks and infrastructures. Allies will report on their progress as of 2017. Together with the continuous adaptation of NATO's cyber defence capabilities, this is reinforcing the cyber defence and overall resilience of the Alliance.

Cyber-attacks against NATO

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

Suspicious events are detected every day, and most of them are dealt with automatically. Some require analysis and response by NATO's cyber defence experts. In total, in 2016 NATO experienced an average of 500 incidents per month – an increase of roughly 60% over 2015. This shows 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 to NATO are also helping the Alliance to improve cyber defences.

The **NATO Cyber Range** in Tartu, Estonia, is used by cyber experts to build 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. Although it is not part of NATO 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 defence-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, and NATO engages with countries, 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 – sharing information between cyber crisis response teams, exchanging best practices, etc.

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. It supports NATO's efforts to protect its 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 5041
E-mail: moc@hq.nato.int
Follow us @NATOpress

www.nato.int

0686-17 NATO Graphics & Printing