October 2013

NATO Cyber Defence

Increasing Threat

NATO relies heavily on its information and computer systems to conduct operations and pass sensitive or classified data. Like many banks, media or political institutions, NATO is experiencing a growing intensity and frequency of cyber attacks. Threats range from common, low-level malware to highly visible denial of service attacks or invisible but more serious attempts at cyber espionage. Since the 2010 Lisbon Summit the Alliance has been enhancing its cyber defences with new technologies and manpower.

What is NATO doing on Cyber Defence?

The Alliance's top priority is to protect its own networks against cyber attacks. At the core of this defensive effort is the Alliance's cyber defence centre, known as the "NATO Computer Incident Response Capability Technical Centre" (NCIRC TC). The Centre provides technical and operational cyber security services. The NCIRC processes millions of security events per day resulting, including serious cases requiring active follow by cyber defence experts. The Centre is currently undergoing a 58 million EUR major upgrade, which was awarded in March of 2012, to provide state-of-the-art sensors, scanners and intelligent analytic capabilities to better prevent, detect and respond to cyber threats. This upgrade will significantly enhance NATO's ability to protect its own networks. The NCIRC has proven to be a vital hub for dealing with cyber incidents and for disseminating cyber security information across the Alliance. As part of the upgrade, NATO is standing-up two Rapid Reaction Teams that can help protect NATO networks in the event of an attack. NATO's cyber defence work is purely defensive and as the cyber threat continues to evolve, so will NATO cyber defence capabilities.

Integrating Cyber Defence into Defence Planning

Allies also agreed at the Lisbon Summit that cyber defence and relevant capabilities need to be included in NATO's Defence Planning Process (NDPP). In June of 2013 NATO Defence Ministers approved the initial integration of cyber defence capability targets into the NDPP. This process will help to harmonize important work on cyber policy and procedures within NATO and at the national level to ensure that the Alliance's overall cyber defence capability meets agreed targets.

NATO Support to Allies

Allies are responsible for developing their own national cyber defence capabilities and for protecting their own networks. NATO can assist in this process, for example, by sharing expertise and information with and between Allies, by promoting coordination and cooperation and facilitating capability development in this domain, through the NATO Defence Planning Process and through Multinational Smart Defence Projects.

Cyber Defence Training

To build effective cyber defence capacity, Allies agree that it is necessary to invest in technology and to develop appropriate expert skills. Cyber defence has been incorporated into NATO exercises ranging from the strategic level in the Crisis Management Exercise series (CMX) to NATO

Response Force exercises such as Steadfast Jazz, where commanders face complex and realistic cyber attacks as part of the exercise scenario. In addition, there are also dedicated cyber defence exercises for NATO and national cyber experts such as Cyber Coalition and the NATO Cooperative Cyber Defence Center of Excellence's exercise Locked Shields. NATO is also working with Allies to increase the number of cyber awareness courses at NATO Schools and elsewhere.

Cooperation

Cyber threats do not recognize international borders and multinational responses are needed. That is why NATO cooperates with selected partner countries and international organizations on a case-by-case basis in order to share best practices and to conduct joint training and exercises.

The November 2013 NATO Cyber Coalition exercise will bring together cyber defence experts from NATO Allies, six partner countries and the European Union to practice together and enhance interoperability and common practices. Cooperation with industry is also key, given that the private sector owns and operates an estimated 80 percent of the information infrastructure worldwide and therefore represents an important partner for NATO and its cyber defence efforts.

Sharing Cyber Expertise

The NATO-accredited Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia is an international research centre. The centre's main task is to enhance NATO's collective cyber defence capability by allowing Allies to share experiences and best practices, and by providing training and conducting research. The centre is funded by its sponsoring Allies (Estonia, Latvia, Lithuania, Germany, Hungary, Italy, Poland, Slovakia, Spain, the Netherlands and the United States) and is not part of the NATO command structure but its work is important to the Alliance.

Public diplomacy division (PDD) - press and media section
Tel.: +32(0)2 707 1010/1002
Email: moc@hq.nato.int

#NATO #DefMin

1799-13 NATO Graphics & Printing