Defending against cyber attacks

NATO is continuously developing and enhancing the protection of its communication and information systems against cyber attacks. These efforts, and capabilities to assist nations' to protect their networks againts a major attack, represent the practical implementation of NATO's current policy on cyber defence, which was approved by the member nations in January 2008, following the cyber attacks targeted Estonia, in 2007.

The 2010 NATO Summit in Lisbon placed cyber security at the forefront of the new security challenges that NATO and its new Division on Emerging Security Challenges, will have to deal with in the years ahead. Both the new Strategic Concept and the Lisbon Summit Declaration make clear that the rapid evolution and growing sophistication of cyber attacks make the protection of Allies' information and communications systems an urgent task for NATO on which its future security depends. The Summit issued further political guidance and tasking on cyber defence requesting an in-depth review of current policy, relevant updates and an action plan for the implementation of the new policy.

In March 2011 the framework for a Concept on NATO's Cyber Defence was agreed by NATO defence ministers. This will act as a starting point for reviewing NATO's Cyber Defence Policy by June 2011.

- **NATO's cyber defence policy and activities**

Context and evolution

Though NATO has always been protecting its communication and information systems, the 2002 Prague Summit included this function on the political agenda. Building on the technical achievements put in place since Prague, Allied leaders reiterated the need to protect these information systems at their Summit in Riga in November 2006.

A series of major cyber attacks on Estonian public and private institutions in April and May 2007 prompted NATO to take a harder look at its cyber defences. At their meeting in June 2007 Allied Defence Ministers agreed that urgent work was needed in this area. Pursuant to this agreement,

NATO conducted a thorough assessment of its approach to cyber defence and reported back to Ministers in October 2007.

This report recommended specific roles for the Alliance as well as the implementation of a number of new measures aimed at improving protection against cyber attacks. It also called for the development of a NATO cyber defence policy.

Since the cyber attacks against Estonia in 2007, cyber threats have rapidly evolved in frequency and sophistication. In the summer of 2008, the war in Georgia demonstrated that cyber attacks have become a major component of conventional warfare. The development and use of destructive cyber tools that can threaten national and Euro-Atlantic security, represents a strategic shift that has increased the urgency for a new NATO cyber defence policy and a strengthening of defences.

Both the new Strategic Concept and the Lisbon Summit Declaration make clear that the rapid evolution and growing sophistication of cyber attacks make the protection of Allies' information and communications systems an urgent task of NATO on which its future security depends.

The 2010 NATO Lisbon Summit in particular has mandated development of a new NATO policy on cyber defence and an action plan by end June 2011 for its implementation.

NATO will use also its defence planning processes in order to promote the development of Allies' cyber defence capabilities, to assist individual Allies upon request, and to optimize information sharing, collaboration and interoperability. Allies will also work to support the development of international norms of behaviour in cyberspace.

To address the security risks emanating from cyberspace, NATO will work closely with other actors, such as the UN and the EU.

Principal cyber defence activities

Coordinating and advising on cyber defence

The cyber defence policy is implemented by NATO's political, military and technical authorities, as well as by individual Allies. A main aspect of the policy was the establishment of a NATO Cyber Defence Management Authority (CDMA) with the sole responsibility for coordinating cyber defence throughout NATO Headquarters and its associated commands and agencies and moving the existing multiple cyber networks to a centrally managed system. The NATO CDMA is managed by the Cyber Defence Management Board, which comprises the leaders of the political, military, operational and technical staffs in NATO with responsibilities for cyber defence. It constitutes the main consultation body for the North Atlantic Council on cyber defence and provides advice to member states on all main aspects of cyber defence. NATO CDMA operates under the auspices of the Emerging Security Challenges Division in NATO HQ (i.e. Chairmanship and staff support).

Assisting individual Allies

Prior to the cyber attacks on Estonia in 2007, NATO's cyber defence efforts were primarily concentrated on protecting the communication systems owned and operated by the Alliance. As a result of the attacks, which were directed against public services and carried out throughout the internet, NATO's focus has been broadened to the cyber security of individual Allies. This implies that NATO has developed mechanisms for assisting those Allies who seek NATO support for the protection of their communication systems, including through the dispatch of Rapid Reinforcement Teams (RRTs) However, the Allies themselves continue to bear the main responsibility for the safety and security of their communication systems. NATO requires a reliable and secure supporting infrastructure from Allies. Therefore it will work with national authorities to develop principles and criteria to ensure a minimum level of cyber defence where national and NATO networks inter-connect.

Research and training

The "Cooperative Cyber Defence Centre of Excellence (CCDCOE) in Tallinn, Estonia, which was accredited as a NATO CoE in 2008, conducts research and training on cyber warfare and has a staff of 30, including specialists from the sponsoring countries. Further information on CCD COE can be accessed at www.ccdcoe.nato.int

Cooperating with partners

NATO is developing practical cooperation on cyber defence in accordance with the Council Guidelines for Cooperation on Cyber Defence with Partners and International Organisations (approved in August 2008), and the Framework for Cooperation on Cyber Defence between NATO and Partner countries (approved in April 2009).

The CDMA, supported as necessary, by the Civil Communication Planning Committee, the Centres of Excellence on Cyber Defence in Tallinn, Estonia, and on Defence against Terrorism in Ankara, Turkey, as well as NATO's Science for Peace and Security Programme, has held experts' staff talks, fact-finding missions, training seminars, and exchanges of information with interested partners and international organizations (i.e. the European Union and the Organization for Security and Co-operation in Europe).

- ## The principal decision-making and advisory bodies

The North Atlantic Council – NATO's top political decision-making body - has overall control over NATO's policies and activities with regard to cyber defence.

The Defence Policy and Planning Committee (DPPC), which replaced the disbanded Executive Working Group in June 2010, has developed policy level proposals (i.e. preparation of a NATO Policy on Cyber Defence and a NATO decision on the creation of NATO CDMA) for the approval of the Council.

The NATO Consultation, Control and Command (NC3) Board constitutes the main body for consultation on technical and implementation aspects of cyber defence.
The NATO Military Authorities (NMA) and NATO's Consultation, Control and Command Agency

(NC3A) bear the specific responsibilities for identifying the statement of operational requirements and acquisition and implementation of NATO's cyber defence capabilities.

The NATO Communication and Information Services Agency (NCSA), through its NCIRC Technical Centre, is responsible for provision of technical and operational cyber security services throughout NATO. NCIRC has a key role in responding to any cyber aggression against the Alliance. It provides a means for handling and reporting incidents and disseminating important incident-related information to system/ security management and users. It also concentrates incident handling into one centralized and coordinated effort, thereby eliminating duplication of effort.