Defending the networks

The NATO Policy on Cyber Defence

2011

The Cyber Defence Policy at a glance

- Integrate cyber defence considerations into NATO structures and planning processes in order to perform NATO's core tasks of collective defence and crisis management.
- Focus on prevention, resilience and defence of critical cyber assets to NATO and Allies.
- Develop robust cyber defence capabilities and centralise protection of NATO's own networks.
- Develop minimum requirements for cyber defence of national networks critical to NATO's core tasks.
- Provide assistance to the Allies to achieve a minimum level of cyber defence and reduce vulnerabilities of national critical infrastructures.
- Engage with partners, international organisations, the private sector and academia.

Background

The security environment of the twenty-first century has changed remarkably. Our modern societies and economies are wired together by networks, cables and the IP addresses of our computers. Increasingly dependent on complex critical communication and information systems (CIS), the Alliance must adapt and enhance its defences in order to confront emerging challenges head-on. To this end, the revised NATO Policy on Cyber Defence sets out a clear vision of how the Alliance plans to bolster its cyber efforts.

The 2010 NATO Strategic Concept highlighted the need to "develop further our ability to prevent, detect, defend against and recover from cyber-attacks…". Threats are rapidly evolving both in frequency and sophistication. Threats emanating from cyberspace – whether from states, hacktivists or criminal organisations, among many others – pose a considerable challenge to the Alliance and must be dealt with as a matter of urgency.

Why a NATO Policy?

The new NATO Policy on Cyber Defence provides a solid foundation from which Allies can take work forward on cyber security. The document clarifies both NATO's priorities and NATO's efforts in cyber defence – including which networks to protect and the way this can be achieved.

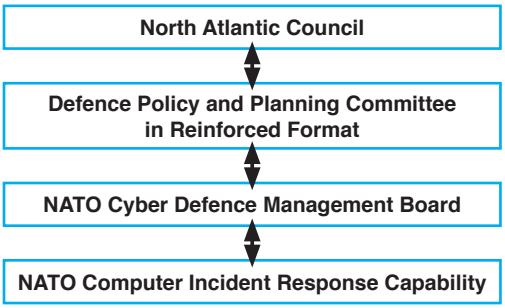
Against this background, at the 2010 Lisbon Summit, the Heads of State tasked the North Atlantic Council to develop a revised NATO cyber defence policy. A NATO Concept on Cyber Defence was first drafted for Defence Ministers in March 2011, which formed the conceptual basis of the revised NATO Policy on Cyber Defence. The Policy itself was then developed and approved by the NATO Defence Ministers on 8 June. The document is coupled with an implementation tool – an Action Plan, which represents a detailed document with specific tasks and activities for NATO's own structures and Allies' defence forces.

Policy Overview

Focus

In order to perform the Alliance's core tasks of collective defence and crisis management, the integrity and continuous functioning of its information systems must be guaranteed. NATO's principal focus is therefore on the protection of its own communication and information systems. Furthermore, to better defend its information systems and networks, NATO will enhance its capabilities to deal with the vast array of cyber threats it is currently faces.

Cyber Defence Governance



Objectives

NATO will implement a coordinated approach to cyber defence that encompasses planning and capability development aspects in addition to response mechanisms in the event of a cyber attack. To achieve this, NATO will incorporate and integrate cyber defence measures across all Alliance missions. For cyber defence capability development, the NATO Defence Planning Process (NDPP) will guide the integration of cyber defence into national defence frameworks. Recognising that NATO requires a secure infrastructure upon which it can operate, NATO networks, including NATO agencies and NATO missions abroad, will be brought under centralised protection. NATO will also develop minimum

requirements for those national networks that are connected to or process NATO information. To achieve this, NATO will identify its critical dependencies on the Allies' national information systems and networks and will work with Allies to develop minimum cyber defence requirements. NATO requires a secure infrastructure on which it can operate, therefore it is important that Allies ensure the protection and defence of national critical information systems and networks. If requested, NATO will assist Allies in achieving a minimum level of national cyber defence.

Principles

NATO cyber defence efforts are based on the overarching principles of prevention and resilience and non-duplication. Prevention and resilience are particularly important given the reality that certain threats will persist despite all efforts to protect and defend against them. Preventing such attacks from occurring in the first place will be achieved by increasing our level of preparedness and mitigating risk by limiting disruptions and their consequences. Resilience is key because it facilitates rapid recovery in the aftermath of an attack.

What is NATO's role in cyber defence?

The main focus of the NATO Policy on Cyber Defence is on the protection of NATO networks and on cyber defence requirements related to national networks that NATO relies upon to carry out its core tasks: collective defence and crisis management.

Response

As stated in the Strategic Concept, NATO will defend its territory and populations against all threats, including emerging security challenges such as cyber defence. The NATO Policy on Cyber Defence reiterates that any collective defence response is subject to decisions of the North Atlantic Council. NATO will maintain strategic ambiguity as well as flexibility on how to respond to different types of crises that include a cyber component. NATO will also integrate cyber aspects into NATO Crisis Management procedures, which will guide NATO's response within the context of a larger crisis or conflict.

NATO will provide coordinated assistance if an Ally or Allies are victims of a cyber attack. To facilitate this, NATO will enhance consultation mechanisms, early warning, situational awareness and information-sharing among the Allies. To facilitate these activities, NATO has a framework of cyber defence Memoranda Of Understanding in place between Allies' national cyber defence authorities and the NATO Cyber Defence Management Board.

For incident response within NATO's own information infrastructure, NATO Computer Incident Response Capability (NCIRC) takes care of the day-to-day business and applies appropriate mitigation measures.

How will NATO respond in the event of a cyber attack on NATO or the Allies?

Any collective defence response by NATO will be subject to political decisions of the North Atlantic Council. NATO does not pre-judge any response and therefore maintains flexibility in deciding a course of action that may or may not be taken.

Engaging the International Community

Cyber threats transcend state borders and organisational boundaries. Their vulnerabilities and risks are shared by all. Recognising the truly global nature of cyberspace and its associated threats, **NATO and Allies will work with partners, international organisations, academia and the private sector** in a way that promotes complementarity and avoids duplication. NATO will tailor its international engagement based on shared values and common approaches. Cooperation in the field of cyber defence could encompass activities including awareness-raising and sharing of best practices.

Practical Steps

- NATO will develop minimum requirements for those national information systems that are critical for carrying out NATO's core tasks.
- NATO assists Allies in achieving a minimum level of cyber defence in order to reduce vulnerabilities to national critical infrastructure.
- Allies can also offer their help to an Ally or to the Alliance in case of a cyber attack.
- Cyber defence will be fully integrated into the NATO Defence Panning Process. Relevant cyber defence requirements will be identified and prioritised through the NDPP.
- NATO Military Authorities will assess how cyber defence supports performing NATO's core tasks, planning for military missions, and carrying out missions.
- Cyber defence requirements for non-NATO troop contributing nations will also be defined.
- Strong authentication requirements will be applied. The acquisition process and supply chain risk management requirements will be streamlined.
- NATO will enhance early warning, situational awareness, and analysis capabilities.
- NATO will develop awareness programs and further develop the cyber component in NATO exercises.
- NATO and Allies are encouraged to draw on expertise and support from the Cooperative Cyber Defence Centre of Excellence in Tallinn.

1368-11 NATO Graphics & Printing