# Towards a European Cyber Defence Policy

**Michael GAHLER**

*Member of European Parliament and spokesperson on security and defence of the EPP Group in the European Parliament*

The rapid evolution of cyberspace in the last two decades not only fundamentally changed our way of living and has offered vast economic opportunities, it also confronts us with new security challenges. The dependence of public infrastructure and global economic relations on availability of, secured access to and stability of cyberspace makes our societies vulnerable at a new level. This new dimension of vulnerabilities was clearly illustrated by the cyber-attacks in Estonia in 2007 and on the European institutions in 2011. Furthermore, in the light of hybrid warfare, as we can experience these days, cyberspace also transforms into a fifth domain of warfare. Considering additionally that cyber infrastructure poses the backbone of any military operation and its success, the issues of cybersecurity and in particular of cyber defence become even more severe. In the past years the EU has started to actively address this issue of cyber defence. The initiatives taken so far can be considered as a starting point for a common cyber defence policy.

In February 2013 the EU took an important step by publishing its cybersecurity strategy in which developing a cyber defence policy was mentioned as one of four priorities. The December 2013 summit on EU´s Common Security and Defence Policy (CSDP) reaffirmed that by recognising cyber defence as a key priority for capability development. Following these events, the Council adopted the EU Cyber Defence Policy Framework (CDPF) in November 2014. This Framework outlines five priority areas for EU cyber defence with special regard to CSDP: supporting the defence capability development related to CSDP, enhancing the protection of CSDP communication networks used by EU entities, promotion of civil-military cooperation and synergies with wider EU cyber policies and relevant institutions, improvement of training, education and exercise opportunities, and finally enhancing cooperation with international partners, especially with NATO.

According to its function as a key actor for capability development in the context of CSDP, the European Defence Agency (EDA) plays an important role in encouraging Member States' cooperation and coordination concerning capability development in cyber defence. Therefore EDA created a project team on cyber defence already in 2011. Furthermore, EDA works in close cooperation with the Member States and other EU bodies and institutions engaged in the issues of cybersecurity and defence, especially the EU Military Staff, the 2004 founded European Network Information Security Agency (ENISA) and the Commission. For example, EDA is participating in several cyber security projects launched by the Commission to evaluate their possible dual-use opportunities.

Although the CDPF and the initiatives of EDA pose important elements of progress towards a common European cyber defence policy, cyber defence still remains one of the most critical areas of shortfalls in capability development as stated by the annual report on CSDP. The projects launched by EDA mainly focus on training while the operational dimension of CSDP is still not comprehensively addressed as envisaged by the CDFP. In particular, a unified cyber defence concept for CSDP covering military operations and civilian missions is not yet formulated and the feasibility assessment of a cyber-defence training facility for CSDP remains to be completed. Likewise no CSDP exercise entirely dedicated to cyber defence has been conducted yet. For the time being there are only plans to include cyber aspects into the CSDP exercises MILEX 2015 and Multi Layer 2016. In comparison ENISA conducted pan-European cyber security exercises in 2010, 2012 and 2014. Furthermore, promotion of a single market for cyber security products and fostering research and development as mentioned in the cybersecurity strategy needs to be intensified. This is especially necessary with regard to the development of the European Defence Technological Industrial Base thus reducing the risk of dependency on suppliers outside Europe.

Beyond the measures taken so far, there are additional issues that need open-minded discussions in the near future. First, since cyber defence capabilities evolved to an essential asset for crisis management, the option of developing cyber defence as an active, EU-owned capability for CSDP missions and operations should be thoroughly investigated. While the EU bodies could provide the infrastructure of such a cyber defence center, Member States would be required to deploy the necessary staff. Second, an open-minded dialogue concerning the development and potential use of offensive cyber capabilities as means of achieving operational goals within CSDP should be initiated. For example, cyber capabilities could be used to disrupt the communication of human traffickers in Libya to support the objectives of the EU naval operation Sophia off the Libyan coast. Third, the increasing utilization of cyberspace and social networks for information warfare as a central part of hybrid strategies demands the EU to develop a comprehensive strategic counter narrative addressing the external as well as the internal audience. This issue should be reflected in detail within the forthcoming framework on countering hybrid threats. Finally, following the invocation of the Mutual Defence Clause Article 42.7 after the devastating terrorist attacks in France and with regard to NATO's recognition of cyber-attacks as a case for Article 5 in Wales 2014, the upcoming debate on the Mutual Defence Clause of the EU should also take cyber-attacks into account.