

The "Cybersecurity Act" and the future role of ENISA from a German national perspective

Vice President Dr. Gerhard Schabhüser, Federal Office for Information Security

About BSI:

The Federal Office for Information Security (BSI) is the German national cyber security authority. BSI's mission is shaping information security in digitisation through prevention, detection and reaction for government, business and society. The BSI has a long-standing experience in computer security since its foundation back in 1991.

Today, the BSI is responsible for operational cyber security, for IT standardisation and certification, digitisation as well as crypto development and evaluation. Furthermore, the BSI does consulting work for government, business and society to achieve a common objective: high IT security standards and improving the state of cyber security in Germany.

Summary:

The speech highlights the achievements of the European Union Agency for Network and Information Security (ENISA) since 2004 and draws recommendations for the upcoming mandate negotiation according to the "Cybersecurity Act"¹. As a national cybersecurity agency the BSI values the contribution of ENISA to the EU cybersecurity landscape and highlights that ENISA should support primarily and, where this is deemed necessary, complement the work of Member States (MS) and EU institutions to improve network and information security (NIS) across the EU. The BSI also appreciates the fact that the mandate incorporates ENISA's role in implementing the NIS directive being mandated with supporting tasks in the CSIRT Network as well as supporting the work of the Cooperation Group. In particular, the proposed permanent mandate for the agency as well as the staff increase is highly supported.

However, the "Cybersecurity Act" proposes also tasks for the Agency which are related to the operational cooperation including a role in cyber crisis management as well as building up own capacities for analysing vulnerabilities and incidents. Furthermore, the Agency is intended to get a central role in the newly proposed cybersecurity certification framework. Although appreciating the closer collaboration in tackling large scale cyber incidents on a European scale, Germany questions such a drastical move towards a more operational agency due to the following reasons:

- Cyber security capacities and competences mainly lie with the MS. A consistent EU cyber security policy must continue to support MS in building their capacities which an operational role of ENISA might hamper. Especially, in the field of operational cyber security trust and vicinity (on a national scale) is of paramount importance, including business and societal actors as well as for critical infrastructures.
- The European cyber security landscape is already equipped with operational actors having their own responsibilities and tasks related to the NIS of Union institutions and respective agencies. First and foremost, CERT-EU which provides operational services to its constituents is participating in the CSIRT Network being initiated by the NIS Directive. With respect to cyber crisis management, a cyber crisis follows the same rules as any crisis with a primary responsibility for the MS. Established mechanisms for a crisis provide for ways to reach a joint understanding within the EU on the basis of national assessments ("common situational awareness"). They also apply to large-scale crises and significant cyber incidents. Prescriptive rules to engage ENISA or any other European actor decreases the functionality of the CSIRT Network.
- An ENISA - also with increased staff and better financial possibilities - can neither substitute nor replace adequate national cybersecurity authorities.

Germany supports an ENISA with a strengthened mandate mainly being based on a deepening of its existing tasks and a realistic approach towards new tasks. In particular, this applies to the foreseen role of ENISA in the set-up of a future cybersecurity certification framework.

¹ Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on ENISA, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")