Analyses OSW

CENTRE FOR EASTERN STUDIES 2.03.2011 www.osw.waw.pl

Germany adopts a cybernetic security strategy

On 23rd February the German government adopted a cybernetic security strategy. Germany plans an increased counteraction against cybernetic attacks of criminal, terrorist and intelligence origin. Germany is concerned about the increase of industrial espionage that afflicts German companies to an ever greater extent, the increase of the number of cyber attacks on IT networks of the federal administration and the appearance of programs that may threaten the critical IT infrastructure in Germany (e.g. Stuxnet, which influenced the operation of Siemens software controlling production lines, power plants and pipelines in Iran).

According to the last counterintelligence report for 2009 on security threats in Germany, companies and institutions in Germany are most frequently attacked from China and Russia.

The strategy's objective is to develop an integrated civil approach to the issue of cybernetic security. The government's aim is to improve: (1) the security of the critical IT infrastructure in the energy, telecommunications, transport and water management sectors; (2) the security of IT systems used by German citizens and by small and medium businesses; (3) ITC security in federal and land administration. The further development of existing software (e.g. KRITIS in case of critical IT infrastructure), an extension of the IT offer for small and medium businesses and the creation of a single and secure network infrastructure for the federal administration are being planned. On top of this the government wants to create a National Centre for Cybernetic Security whose job would be to improve the cooperation of all government structures dealing with this problem, and to coordinate programs securing IT infrastructure. Also, a National Council of Cybernetic Council is to come into being. The task of this organisation would be strategic prevention planning and most ministries and representatives of the German economy are to cooperate within it. Moreover, actions on the EU and international level have been announced, including endeavours to extend the mandate of the *European Network and Information Security Agency* (ENISA), to support the use of unified standards by NATO also in civil critical IT infrastructure and to develop an international code of conduct in cyberspace.

<jus>