

## CEPIS Calls for European Best Practice Framework on Cybersecurity

BRUSSELS, BELGIUM, June 13, 2018

CEPIS' Legal and Security Issues Special Interest Network (LSI SIN) has published a new paper, *Best Practices for a Journey Towards Secure Cyberspace*, which evaluates the approach of different National Cybersecurity Strategies (NCSS) within the EU. The paper calls for a common European evaluation framework to help ensure the long-term aim and success for reducing risks to cybersecurity among EU member states.

According to the newly released paper, the current assessment by the European Union Agency for Network and Information Security (ENISA) of European NCSS does not sufficiently address broader, political-strategic aspects that are essential for securing the common cyberspace. ENISA's assessment mainly focused on operational issues, such as incident management and awareness raising, while any efforts for improving the high-level decision-making capacity needed for long-term success are not included.

"In order to bring Europe's industries safely into the digital era and provide the space for them to thrive, effective national strategies that encompass cybersecurity at every level are a must," it was stated by Prof. Dr. Kai Rannenberg, of CEPIS' LSI SIN.

For this reason, a new, common European framework for evaluating individual national strategies has been proposed by the group, which also suggests examining the Member States' NCSS according to four, specific domains and how well they comply with them. These are listed below:

1. Setting up a specific body for coordinating efforts at the political-strategic level
2. Active cooperation with the international community to address transnational cybersecurity issues
3. Development of industrial and technological resources for the international cybersecurity ecosystem, such as highly secure products or innovative approaches
4. Initiating efforts to reduce cybercrime

Using this approach, the paper also concludes that 38% of 21 analysed European NCSS currently fail to represent a holistic approach to cybersecurity, and that they should apply new methods for assessing and monitoring the institutions dealing with cybersecurity. It is further noted that many of the national institutions that handle cybersecurity enforcement are still dependent on the state, which is problematic as the state institutions are stakeholders themselves and should be separated from the pertaining authority of cybersecurity. [The full paper may be found here through the CEPIS website.](#)

-ENDS-

---

## ABOUT CEPIS

The Council of European Professional Informatics Societies (CEPIS) is a non-profit organisation seeking to improve and promote a high standard among ICT professionals, in recognition of the impact that ICT has on employment, business, and society. CEPIS currently represents 33 member societies in 32 countries across greater Europe. Through its members, which are the professional ICT bodies at national level, CEPIS represents 450,000 ICT professionals. Established in 1989, CEPIS has since grown to become the independent authority on - and network for - ICT Professionalism in Europe.

---

## CONTACT DETAILS

Ulrik Lorck - Communication Officer

Tel.: +32 (0)2 770 7113

Email: [ulrik.lorck@cepis.org](mailto:ulrik.lorck@cepis.org)