

EU must continue to guarantee highest hardware resistance levels to cyberattacks

Written by Stéphane Mouille on 4 June 2018 in Thought Leader
Thought Leader

Europe must continue to guarantee the highest hardware resistance levels to cyberattacks, says Stéphane Mouille.



Europe's leadership in digital security was established thanks to the unique expertise and knowledge developed in the Senior Officials Group - Information Security Systems Mutual Recognition Agreement (SOG-IS MRA) certification scheme which has now been operational for more than 25 years.

EU policymakers - as they debate the details of the so-called Cybersecurity package - are currently looking at how Europe can combat cybersecurity attacks. Europe is the undisputed worldwide leader in guaranteeing the highest resistance levels to potential attacks, thanks to the unique expertise and knowledge developed under the SOG-IS MRA certification scheme.

The scheme has a long and proud history and its principles are based on several key factors, such as the ability of security evaluation laboratories to perform ethical hacking and penetration testing while

evaluating products, services or solutions.

RELATED CONTENT

- [Angelika Niebler: EU can become a leading player in cybersecurity](#) [1]
 - [MEPs give cautious welcome to EU cybersecurity proposals](#) [2]
 - [Julian King: Bold EU action is required to address cyber vulnerabilities](#) [3]
 - [Elissavet Vozeberg-Vrionidi: It's time for cyber-justice](#) [4]
 - [Jorge Domecq: Cyber-defence: The new security challenge](#) [5]
-

Security evaluation laboratories also share a uniform level of evaluation, thanks to peer-reviews performed by EU member states' national security agencies. Mutual certification recognition among all SOG-IS MRA members is also key.

Originally created by Eurosmart, the JHAS ethical hacking group is renowned for its expertise, intelligence and strong savoir faire. It is now the worldwide reference for blue chip companies such as Qualcomm, Visa, MasterCard, Samsung... and of course all the Eurosmart members.

We also have a successful track record in developing this unique European expertise. Prestigious organisations such as Nato, DHS, SWIFT, Visa, MasterCard, Microsoft, high-end smartphone manufacturers, Audi, Mercedes, Barclays, Airbus and Google all use Eurosmart technologies certified in Europe through the SOG-IS MRA certification scheme.

As President of Eurosmart, I want to reiterate the need to protect Europe through cybersecurity and to restate our five outcome-based principles.

First, clear legal definitions of essential terms referring to IT and security ecosystems.

Second, fair and open European governance during the preparation phase of candidate European certification schemes.

Third, a well-defined European certification objective that is appropriate for each level of certification. Above all, EU co-legislators should ensure that the 'substantial' and 'high' levels require mandatory Ethical Hacking testing (Penetration testing) by Conformity Assessment bodies (CABs) during evaluation.

Fourth, European standards must be the basis for the preparation of a new candidate European certification scheme.

Last, the EU Agency for Network and Information Security's, (ENISA) 'Intellectual Property Rights (IPR policy) should be spelled out in the cybersecurity act.

We urge the European Parliament, Commission, and Council to introduce the SOG-IS MRA certification schemes into the initial text - as an appendix to the Cybersecurity act regulation - to avoid any risk of disruption in European excellence and to make ethical hacking mandatory during substantial and high-level evaluations.

[**Download the new Eurosmart policy paper, 'Cybersecurity Act: Ethical hacking does matter!'**](#) [6]

About the author

Stéfane Mouille is President of Eurosmart the European digital security industry association

Tags

[Digital Agenda](#) [7]

[Research and Innovation](#) [8]

Categories

[Business and industry](#) [9]

[Data privacy](#) [10]

[Digital single market](#) [11]

[Science, technology and research](#) [12]

Twitter Link

Read more on:

[Facebook](#) [13]

[Twitter](#) [14]

[Website](#) [15]



Site Sections

- [Home](#)
- [Content](#)
- [Policy](#)
- [Magazines](#)
- [PM+](#)
- [Thought Leader](#)
- [EU Elections 2019](#)
- [Editorial Calendar](#)
- [Policy Events](#)
- [Event Coverage](#)
- [MEP Awards 2019](#)
- [Contact Us](#)

Services

[Dods PeopleDods](#)

[MonitoringDods](#)
[ResearchDods](#)
[EventsDods](#)
[Training](#)

Media & publishing titles

[Politics HomeThe HouseThe Parliament](#)
[MagazineHolyrood](#)
[Total PoliticsPublic Affairs NewsCivil Service World](#)
[PublicTechnology Training JournalDods Parliamentary CompanionVacher's Quarterly The European Union and Public Affairs Directory](#)

Dods events

[Westminster BriefingDigital Health & Care ScotlandMEP AwardsThe Skills SummitScottish Public Service AwardsPublic Sector Procurement SummitPublic Sector ICT SummitCyber Security SummitCyber Security 2017Training Journal Awards](#)

Partnership events

[The Health and Care Innovation ExpoCivil Service](#)

[LiveCivil Service](#)
[AwardsChief](#)
[Nursing Officer for](#)
[England's](#)
[SummitWomen into](#)
[LeadershipThe](#)
[Youth Justice](#)
[ConventionSocitm](#)
[Spring](#)
[ConferenceNHSCC](#)
[Annual Members'](#)
[EventDods at Party](#)
[Conference](#)

[Privacy Policy](#)[Terms & Conditions](#)[Advertising](#)[Sponsorship](#) [Subscriptions](#)

Source URL: https://www.theparliamentmagazine.eu/articles/partner_article/euro-smart/eu-must-continue-guarantee-highest-hardware-resistance-levels

Links

- [1] <https://www.theparliamentmagazine.eu/articles/opinion/eu-can-become-leading-player-cybersecurity>
- [2] <https://www.theparliamentmagazine.eu/articles/opinion/meps-give-cautious-welcome-eu-cybersecurity-proposals>
- [3] <https://www.theparliamentmagazine.eu/articles/interviews/julian-king-bold-eu-action-required-address-cyber-vulnerabilities>
- [4] <https://www.theparliamentmagazine.eu/articles/opinion/its-time-cyber-justice>
- [5] <https://www.theparliamentmagazine.eu/articles/opinion/cyber-defence-new-security-challenge>
- [6] <https://www.theparliamentmagazine.eu/whitepaper/euro-smart/eurosmart-cybersecurity-policy-paper>
- [7] <https://www.theparliamentmagazine.eu/tags/digital-agenda>
- [8] <https://www.theparliamentmagazine.eu/tags/research-and-innovation>
- [9] <https://www.theparliamentmagazine.eu/categories/business-and-industry>
- [10] <https://www.theparliamentmagazine.eu/categories/data-privacy>
- [11] <https://www.theparliamentmagazine.eu/categories/digital-single-market>
- [12] <https://www.theparliamentmagazine.eu/categories/science-technology-and-research>
- [13] <https://www.facebook.com/TheParliamentMagazine/>
- [14] <https://twitter.com/parlimag>
- [15] <http://www.theparliamentmagazine.eu/>