PRESS RELEASE

Stockholm, Sweden
April 17, 2023

Enea Urges EU PEGA Committee: Broaden the focus beyond spyware to combat mobile surveillance threats and signaling infrastructure exploitation.

Enea, a world-leading specialist in telecommunications and cybersecurity software solutions, recently highlighted the types of spyware being used over mobile networks at a public hearing of the European Parliament's PEGA Committee of Inquiry into the use of Pegasus and surveillance.

Rowland Corr, Vice President of Government Relations at Enea, was one of several industry experts invited to share his expertise at the Committee of Inquiry, which consists of 38 Members of Parliament.

The PEGA Committee was formed in March 2022 by the European Parliament to investigate spyware, particularly in relation to the alleged targeting of journalists, lawyers, law enforcement officials, diplomats, and other people of influence in the EU. Corr appeared at the Committee's most recent hearing on March 16, 2023, and prefaced his contribution by urging the Committee to broaden its scope, highlighting the fact that other forms of spying beyond the use of spyware were steadily occurring over mobile networks that were relevant to the Committee's concerns.

"Spyware is the tip of the iceberg in mobile telecom surveillance," Corr commented. "Vulnerabilities in mobile networks, and governance gaps are exploited by threat actors to execute unauthorized intrusions with impunity."

Corr also made the point that capability must be prioritized over mere compliance to combat the threat effectively, as the signaling security landscape continues to evolve over time. He continued, "This area of risk is not sufficiently understood, reported or integrated at national levels . Critical infrastructure protection, cybersecurity, and national security all intersect when it comes to mobile network security. And the key to improving resilience may lie in emphasizing capability over compliance on the part of stakeholders - be they operators, regulators, or cyber agencies."

Recently, the potential for access to EU-based infrastructure to be used by third-country actors as a tool for surveillance, separate from the use of spyware, has increased significantly. Corr continued to impress upon the Committee the importance of looking at surveillance threats beyond the basic use of spyware tools like Pegasus and, in parallel, focus on infrastructure as a whole:

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website:
www.enea.com

“A key area of vulnerability is mobile telecoms signaling and the abuse of access to signaling infrastructure. To put this vulnerability into context as an area of surveillance risk - the use of mobile spyware weaponizes the personal device of the victim, and the use of mobile signaling weaponizes the network serving them. Put simply, in the hands of attackers, the mobile service itself becomes the cyber weapon.”

As 5G is adopted worldwide, there is a pressing need for secure interworking between protocols, network elements (across generations) and a need for secure interconnections nationally and internationally. This represents an increasingly complex and critical area within electronic communications.

Enea has received industry recognition as a leader and innovator in mobile telecoms security for protective solutions, research into vulnerabilities, and contribution to the development of industry guidelines. As outlined by the Committee Chair, a core part of Enea’s business is securing networks and protecting subscribers worldwide against unauthorized intrusions.

The PEGA Committee was tasked with gathering information on the extent to which Member States or third countries are using intrusive surveillance to the extent that it violates the rights and freedoms enshrined in the EU’s Charter of Fundamental Rights. The Inquiry has a 12-month mandate, which parliament can extend if required. A report based on the findings of the Inquiry is set to be published later this year.

About Enea

Enea is a world-leading specialist in software for telecom and cybersecurity. The company’s cloud-native solutions connect, optimize, and secure services for mobile subscribers, enterprises, and the Internet of Things. More than 100 communication service providers and 4.5 billion people rely on Enea technologies every day. Enea has strengthened its product portfolio and global market position by integrating a number of acquisitions, including Qosmos, Openwave Mobility, Aptilo Networks, and AdaptiveMobile Security. Enea is headquartered in Stockholm, Sweden, and is listed on Nasdaq Stockholm.

For more information: www.enea.com

Enea AB, P.O. Box 1033
164 21 Kista

Phone: +46 8 507 140 00
Fax: +46 8 507 140 40

E-mail: info@enea.com
Website:
www.enea.com