Abstract

The new 5G technology, next generation of telecommunication and mobile network, is all around the world in course of inspection and inquiry for its astonishing novelty, from new services to functions and scalability. However, every technology brings alongside new possibilities and new threats scenarios, especially in this case where the impact on the present network is promised to be massive, with brand new features allowed by 5G, like Internet of Things, widespread virtualization and huge leap forward in rapidity and capability of the mobile transmission. An increase in the network surface, considered as more connections, more devices connected and more traffic load of data, will expand also the possible entry point and fault exploitable by a malevolent actor, raising common concern about the technology. The deployment of such a technology on European soil, especially in some states of the Union, caused uproar and critics primarily in the security field. Following a global trend, but also leading a best practice approach, the EU developed a series of mechanisms and agencies that are challenged to oversees the gradual shift from old 4G LTE to 5G. In this paper a Critical Information Infrastructure Protection (CIIP) framework is used to analyse the criticalities of the new technology. Definition of the critical sectors, Regulations and Organization predisposed to cybersecurity, cooperation mechanism will be covered to formulate the possible solution to adopt and thus, minimize the damages to the vital internet network.

Length of the work: 97.000 characters