**The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data**

By Chatziioannou Konstantinos, LLM, PhD candidate, Aristotle University of Thessaloniki, Faculty of Law, Department of Criminal Law and Criminology

The Convention on Cybercrime (Art. 6) and the Proposal for a Directive on attacks against information Systems (Art. 7) intend to introduce to national law the criminalization of the use of tools, such as malicious software and unrightfully obtained computer passwords, for committing crimes against the confidentiality, integrity and availability of information systems and computer data. This goal seems to be ambitious, taking into account the several attacks that take place nowadays against both critical infractures and personal information systems and the necessity of the harmonization of cybercrime law due to its global nature. In the paper it is examined whether the penalization of such preparatory actions is necessary and reasonable from the perspective of the protected legal interest. Referring to the actus reus of the proposed elements of the crime it is examined whether the restriction of the criminalization to devices that are designed or primarily adapted for the purpose of committing any of the offences against the security of the information systems could be delimited and whether it is compatible with the ultima ratio principle. Regarding the intent requirement of the aforementioned proposed crimes it is vital to analyze the possibility of the determination of the purpose of committing an offense against the information systems in a networked digital environment. A main problem that is raised by these provisions is the avoidance of criminal liability in cases where such tools are used for authorized testing of the information systems and therefore strengthen their security. These problems become even worse, when the so called hacking tools refer to dual-use programs.