# SHIELD– Securing against intruders and other threats through a NFV-enabled environment

Nikolaos Papadakis [1], Antonius Litke (Infili Technologies) [2] and Dimitris Papadopoulos [3]

[1,3]Department of Mathematics and Engineering Sciences,
Hellenic Military Academy,GR- 166 73 Vari, Greece

[2]Institute of Communications and Computer Systems (ICCS),
National Technical University of Athens,
9, Iroon Polytechniou Str., GR-157 73 Zografou, Greece

E-mails: [1] npapadakis@sse.gr , [2] ali@telecom.ntua.gr and
[3]dpapadopoulos6@isc.tuc.gr

ABSTRACT

Organisations nowadays are witnessing an unprecedented escalation of cybercrime attacks and struggle to keep the pace to fight them. According to the 2013 Norton Report2, economic losses due to consumer cybercrime -for Europe alone- were estimated at 13 billion dollars. Moreover, Ponemon study3 also points that the tendency of these economic losses is increasing. The sophistication of new attacks, the increasing weakness of traditional security controls and the explosion of data to be collected and analysed to detect threats render evident that most of the security strategies used in the past are increasingly less effective against new and complicated types of attacks. Many tools and

security processes have been more focused on prevention than on detection and response, and attackers are taking advantage of the fact that organizations are not finding the indicators of compromise within their environments soon enough, nor are they responding to these incidents and removing them quickly enough.

The purpose of this paper is to provide an overview of the motivations and technical work carried out by the EU-funded SHIELD project. This project aims at combining Network Functions Virtualisation (NFV), Security-as-a-Service (SecaaS), Big Data Analytics and Trusted Computing (TC) to provide an extensible, adaptable, fast, low-cost and trustworthy cybersecurity solution. Main focus will be given to the conceptual and architectural design of the cognitive Data Analytics and Remediation Engine, which has been the authors' main development task. □