"Tackling Today's Emerging Regulatory Frontiers- Cyber Security, Artificial Intelligence, Internet of Things & Blockchain. Tackling Today's Emerging Regulatory Frontiers- Cyber Security, Artificial Intelligence, Internet of Things & Blockchain"

Excellencies, distinguished colleagues, ladies and gentlemen,
I feel honoured to have the opportunity to contribute to the International Conference on Cyberlaw, Cybercrime & Cybersecurity.

ICT is stimulating changes in the way most people earn their incomes, varying the balance between our roles as consumers and producers, revolutionizing the way we produce and deliver goods, changing the way we educate succeeding generations and train ourselves, transforming the delivery of health care, altering the way we govern ourselves, altering the way we form communities, changing the fruition of the world's cultural heritage, varying the way we obtain and communicate information, contributing to bridge some cultural or physical gaps, modifying patterns of activity among the elderly and perhaps contributing to a greener world.

Cyber technology is pervasive and its key role is growing up every day, citizens consider cyber technology as a commodity. Mobile devices represent the most recent revolution in both technology and society, they are perceived as something different from computers even if they play, among others, the same role and immediately became part of our daily life, a wearable accessory as our wallet or wristwatch. Extremely user friendly devices are nowadays used by formerly digital divided citizens having no idea about potential drawbacks. As a side effect of globalisation and massive cyber services the number of crimes both perpetrated at local and global level is growing up.

The discontinuity ignited by cyber technology and its pervasiveness created the fundamentals for a completely new scenario where the malicious use of digital technologies is becoming a new business opportunity not only as a direct mean to steal "assets" and take control of smart objects but even under the format of "cyber-crime as a service", at the same time terrorists found in cyber technology the best mean both to run their activity and to enrol new "adepts".

The key challenge is to determine what the drivers of new forms of cyber criminality are and how they might be prevented and mitigated. There is a clear need to adopt a renovated set of countermeasures to face and possibly cancel or mitigate such harms. This comprehensive approach requires a strong interdisciplinary methodology ensuring a tight interaction among human factors experts, sociologist, psychologists, cyber-psychologists, anthropologists, technologists and experts in organisational aspects together with lawyers law enforcement agencies and practitioners. To build a sounding information society we must efficiently counteract cyber-criminality and establish a clear vision on legal behaviours in the cyber-world.

It is common knowledge that organizations worldwide face a dangerous shortage of network security personnel that have the skills required to defend against cyber-attacks[1]. At the same time the number of breaches grows steadily, with the incident response and attack defence techniques being time-critical, as the majority of compromises (87%) occurring within minutes[2]. According to the IBM Chief Information Security Officer Assessment, about 95% of all the cyber-

[1] https://www.ixiacom.com/company/blog/benefits-cyber-range-training

[2] https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf

security incidents are caused by human errors. This kind of incidents have a very high impact since they involve employees, that have access to company relevant business information and sensitive data. The most common type of attacks carried out thanks to the human vulnerabilities are reported in Vormetric Inc., White Paper – The Insider Threat, 2013 and they include: exposure of sensitive data, theft of intellectual property and the introduction of malware.

This situation illustrates the problem of lack of preparedness organisations face in defending effectively against cyberattacks. Human factors are also at the root of the design of security strategies and methodologies in the European Security Model that includes the development of a common understanding of security issues among EU security practitioners , as well as of the causes and effects of insecurity among EU citizens.

Internet users in the EU remain very concerned about cybercrime. According to EuroBarometer 2017, a large majority (87%) of European Union citizens regard cybercrime as an important challenge to the internal security of the EU: 56% think that cybercrime is a very important challenge and 31% see it as fairly important (based on more than 28000 face-to-face interviews). In 2015, 80% (42% and 38%, respectively) were of the same opinion.

Today, the increasing complexity of cyber-physical and socio-technical systems due to their continuous enrichment of different types of users (personas), as well as the plethora and variety of devices (such as IoT) requires a strong baseline and a pool of partners with a collective knowhow and established competency in running Cyber Ranges, specialisation in specific application domains (such as Industrial systems, IoT, etc.) and cybersecurity coordination centres (e.g. CERTs/CSIRTs).

Some of the key topics to be considered involve use, misuse, abuse of cyber ecosystem, privacy and data harvesting, fake news, darknet, IoT, machine learning, artificial intelligence, crypto-currencies / fintech, quantum computing, and last but not the least cyber warfare.

The **International Conference on Cyberlaw, Cybercrime & Cybersecu**rity represents an outstanding and unique event to better understand, prevent and fight cybercrimes in a global dimension. ICCC provides an international platform for fruitful dialogue amongst various stakeholders in cyberspace.

Pavan Duggal is the man who timely understood the relevance of cybercrime in nowadays society and had the idea to create the perfect reference point for multidisciplinary experts required in order to deal with it.

Thank you Pavan for this outstanding and unique event. I wish all of us a productive couple of days leading to the development of positive concrete results.

Thank you for your attention.