19 NOVEMBER 18:00
INAUGURAL CEREMONY & NETWORKING DINNER

Excellency, colleagues, ladies and gentlemen, and friends good afternoon,
It is my honour and pleasure to participate to the inaugural ceremony of the Internation Conference on CyberLaw, CyberCrime, CyberSecurity 2025.
I would like to express my thanks to Pavan Duggal and the ICCC team as the originator and manager of the conference. The ICCC is the main reference point in these sectors.
One of the key excellences is the ability to capture and foresee evolving innovation trends in the cyber domain. In the recent editions AI captured the interest of the conference. The evolving digital transition poses some relevant questions and concerns involving the actual and foreseeable impacts on society and citizens.
Future based on a single fragile pillar cyber technology, human rights, ethics, centralisation of power, top down control.

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. On the occasion of the pandemic cybertech represented for a number of activities and situations a real lifeblood.
This global crisis represents a stress test for the actual organisation of society, almost all the social and economic sectors are under pressure due to the pandemic.
The pandemic impacted health, economic, social, phycological, human aspects and more, modifying lifestyle, altering behavioural patterns, perceptions. Limiting, directly or indirectly, freedom; generating a sense of insecurity and real and present danger, amplifying a sense of loneliness in seniors. Resilience is the keyword, "improving resilience" is the general effort in many sectors from education to healthcare including general critical infrastructure.

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. 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 . According to the IBM Chief Information Security Officer Assessment, about 95% of all the cyber-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 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.

Keeping Europeans safe online is a priority for the Commission. The EU has advanced in the fight against cybercrime, with for instance stronger rules against online payment fraud and better assistance to victims. The EU also helps building up the capacity of law enforcement authorities to tackle cybercrime, with the European Cybercrime Centre at Europol supporting Member States by providing tools, expertise, and coordination of police action. More generally, the EU supports Member States’ cybersecurity preparedness and promotes swift and effective cooperation on cybersecurity issues, through a comprehensive legal framework including the Directive on security of network and information systems (NIS Directive), the EU Cybersecurity Act, the European Blueprint.
The NIS Directive is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.
A culture of security across sectors which are vital for our economy and society and moreover rely heavily on ICTs, such as energy, transport, water, banking, financial market infrastructures, healthcare and digital infrastructure. Businesses in these sectors that are identified by the Member States as operators of essential services will have to take appropriate security measures and to notify serious incidents to the relevant national authority. Also key digital service providers (search engines, cloud computing services and online marketplaces) will have to comply with the security and notification requirements under the new Directive.

Respondents worry about misuse of their personal data, fraud, being locked out of their computer and forced to pay ransom to access their own data, as well as about identity theft. More than a third have received fraudulent emails or phone calls asking for personal details in the last three years; 8% fell victim to ransomware, and 11% had their social media account or email account hacked. This has an impact on their willingness to use online services: for example, 10% say their concerns make them less likely to make purchases online. This trend was completely overturned due to the pandemic that boosted the use of on-line shopping from food to health devices.

A consortium of European partners created a proposal for the next generation of a data infrastructure for Europe: a secure, federated system that meets the highest standards of digital sovereignty while promoting innovation. GAIA-X is a project initiated by Europe for Europe. Its aim is to develop common requirements for a European data infrastructure. Therefore openness, transparency and the ability to connect to other European countries are central to GAIA-X. Representatives from seven European countries are currently involved in the project.
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.

Evolution of ICCC from my first participation, improvements, etc.
The International Conference on Cyberlaw, Cybercrime & Cybersecurity 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.
My personal experience on ICCC dates back to 2015 when I received the invitation to contribute to THE INTERNATIONAL JOURNAL ON CYBERLAW, CYBERCRIME & CYBERSECURITY to be published in 2016. My first physical participation to the ICCC Conference was in 2016. The program included 45 cybersecurity topics,

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.