

2023 ICCC Opening Ceremony

Alfredo M. Ronchi
alfredo.ronchi@polimi.it

Today I am very honoured to contribute to the opening ceremony of the tenth International Conference on Cybercrime, Cyberlaws, Cybersecurity. We are back in presence after the last three held in virtual format.

This tenth edition is an important milestone strengthening the improving relevance of these topics through time.

The multi-faceted crisis of 2020-2021 represented a stress test for the organization of society, furthermore, the health crisis has had an impact on economic, social, psychological, human aspects and more, modifying the lifestyle, altering behavioural patterns, perceptions, restricting, directly or indirectly, human rights and freedom, generating a sense of insecurity and setting up a sense of real and present danger, amplifying a sense of loneliness in seniors.

As someone said we will not come back to the previous “normality” we are establishing a “new” normality.

Since the beginning of the pandemic cyber technology was immediately considered the silver-bullet to contribute to mitigate the drawbacks, so during lockdowns e-services mainly devoted to merchandise and food delivery enjoyed an incredible success and several new spinoffs were activated. This completely unusual situation, lockdowns, reduced opportunity to travel, need to find new solutions to perform usual tasks stimulated creativity and brains as it happens in case of crisis so, step by step, different sectors discovered a new horizon.

Public administration services suffered a significant crisis even because both the switch to smart work and the digitisation of procedures was critical, museums and cultural institution “invented” guided virtual tours, curators' lectures, virtual round tables. Schools at different levels switched to distant learning using different platforms, students from primary schools to universities had to adapt to this virtual learning environment created on the fly.

The acceleration in digital transition boosted by the pandemic together with the discontinuity triggered by information technology and its pervasiveness have created the basis for a completely new scenario in which the harmful use of digital technologies is becoming a new business opportunity not only as a direct mean to steal "assets" and taking control of intelligent objects, the 'foul' use of AI and ML by hackers can "weaponise" these advanced technologies, in addition the format of "cyber-crime as a service" was blooming, terrorists have found in cyber-technology the best way both to manage their business and to recruit new "followers".

Recently it appeared that Microsoft basically acquired OpenAI, i.e., former OpenAI leaders Sam Altman and Greg Brockman are now working at MSFT.

After the previous interest in the 1980s the emerging trend concerning AI and ML is generating concerns. If on one side AI will benefit citizens, business and public interests on the opposite side creates some risks for the safety of consumers and users, for fundamental rights, potentially releasing humans from ethical dilemmas.

In addition to virtual interpersonal / social communication-continuity ensured by audio and video connections, online services ranging from e-Gov to shopping and food delivery were master tools for survival in a lockdown status and after this crisis are appreciated even in normal conditions. New e-services were created on the fly to bridge gaps due to the pandemic. The compelling and strong need to take advantage from these cyber-channels lowered the care and attention to security issues, this was a unique opportunity for criminals to sell fake medicines, protections, medical devices, and COVID PASSES or to cheat young and seniors stealing sensitive data.

Limited mobility and emergency-reshaping of protocols pave the way to cheaters, identity thieves, and other malicious people.

If we focus on currency and payments several new services, even proposed as anti-pandemic tools, have been deployed, from the pervasiveness of contactless cards to e-Wallets and smart phone- or wristwatch- based transactions, dramatically reducing the use of traditional currency, bills, and coins.

Digital transition imposes to store, we hope, efficiently managed, and secured, a huge amount of governmental and personal sensitive data in cloud repositories in the format of bit streams.

The advances in “digital transition” and consequent need for cloud storage push governments to put in someone's else “safe hands” a consistent portion of the country, the digital one.

The Global digital compact is the new global agreement to shape the new order.

Resilience was one of the recurring keywords in the recent past, “improving resilience”, this was the general effort in many sectors from education to healthcare including general critical infrastructures. At the same time another keyword was “to secure economy” finding the golden balance between citizens health and economy, let’s say “as open as possible, as closed as much necessary”.

The actual trend of some governments is to open a bid to assign the provision of cloud storage to private business companies, this is even due to the lack of relevant state-owned national cloud infrastructure. This aspect that is tightly related to keywords like cyber sovereignty and even homeland security seems not to be carefully considered nowadays.

Ten years ago cybersecurity was mainly a pillar to enable e-commerce and e-business, today’s ubiquity of cyber technology makes this topic a key part of our daily life.

We are surrounded by “critical infrastructures” managed by cyber components that, in case of attacks, may create mayor or minor impact on our daily life. We don’t mean only typical critical infrastructures like communication, energy, water, health, transportation, and last, but not less important nowadays financial services; due to citizens appreciation and their role as everyday “tools” we can consider among “critical infra-structures” even information services, social media, geo-positioning, home automation, smart cities, safety, and security devices, and more. It will not surprise if in few years big service platforms as GAMAM or food delivery platforms will be considered critical infrastructures. In addition, there is a clear need to reconsider supply chains and their resilience.

To conclude let me spend few words about the event itself and its inventor, organiser, and chair Pavan Duggal; within the global scenario the International Conference on Cyberlaw, Cybercrime & Cybersecurity represents an outstanding and unique event to better understand, prevent and fight cybercrimes in a multidisciplinary global dimension not limited to technological and criminal aspects but directly involving a wide range of experts and stakeholders.

The program shows continuous improvements year by year since the first edition in 2013.

Three days, two plenary tracks, two parallel tracks, two round table track including for the first time CISO track, 41 cybersecurity related topics, and more than 100 international speakers, more than 750 people to attend two-days multi-stakeholder event which consists of Government leaders, representatives from Law Enforcement Agencies, Government bodies, Security Professionals, Lawyers, Jurists, Cybercrime Investigators, Corporate leaders from both Public and Private Sector.

I attended for the first time the ICC Conference in 2016 and I found this event an incredible multi-cultural, multidisciplinary, multistakeholder melting pot of knowledge, ideas, skills, and willingness to cooperate. I found a close and evident connection between this event and the aims and activities of the WSIS, // ICCC can act as a preparatory event not only in the field of action line C5 Building Confidence and Security in the Use of ICTs but even in Ethical, digital transition and more panels.

One of the relevant outcomes of these efforts is the ICCC Academy offering a wide range of training courses, we hope now hosted by the ITU Academy organisation.

All these initiatives and events are due to the expertise and strong commitment of Pavan Duggal, 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 (SSH, philosophers, sociologists, etc) required to deal with it.

Conference Director, Pavan Duggal has been acknowledged as one of the top Four Lawyers in the cyber world. The list of key positions and roles is almost endless as well as the number of workshops, lectures, books, and publications.

Thank you Pavan for your efforts and this outstanding and unique event.

I wish all of us a couple of productive days that lead to the development of positive concrete results.