

Alfredo M. Ronchi
alfredo.ronchi@polimi.it

Thank you chair,

Excellencies, speakers, distinguished colleagues, ladies, and gentlemen / good evening – good morning, good afternoon wherever are you located around the world.

Today I am very honoured to contribute to the opening ceremony of the eleventh International Conference on Cybercrime, Cyberlaws, Cybersecurity.

We reached an important milestone last year “the tenth edition of ICCC”, so we are now entering the next decade of ICCC strengthening the improving relevance of these topics through time.

The present edition, in addition to cybersecurity, poses the focus on one of the most significant trends capturing the interests of citizens and engaging researchers: Artificial Intelligence. The acronym AI is mentioned ten times in the Conference program to depict different scenarios and analyse potential benefits and drawbacks. It often happens that appealing emerging technologies ignite controversial consideration: the silver bullet to solve all human issues or the ultimate generator of negatives.

Since the time of the “Imitation game” article in 1950, up to the end of the 1970s and the early 1980s we were hearing about computers writing their code while running “intelligent” applications, basically auto-instructing themselves. It was the time of “Big Blue”, a chess gaming expert system developed in the middle of the 1980s by Carnegie Mellon University running on a purpose-built IBM supercomputer. Early in the 1980s a typical computer science thesis was dealing with hypertext tools or chess gaming software. That time mass media considered AI on one side a potential step forward for humanity on the other side a kind of Moloch, the cyber instance of evil. Afterwards AI and fuzzy logic improved the “intelligence” of washing machines and video cameras, no more capturing the interest of mass media till recent times because of the wide impact generated by some online applications mainly based on machine learning processing huge data sets to produce “magic” outcomes. This ability to analyse huge dataset almost on the fly, discovering invisible, at human eye, patterns or generating deep fake started again to elicit interest and concerns at different levels.

The concern was: “artificial intelligence design will improve itself to think faster and deeper, then the improved version would improve itself, and so on, exponentially”.

Why were citizens particularly concerned about AI? One of the possible reasons is due to the term “artificial intelligence” that ignited the understanding that there were two “intelligences” one human and another artificial potentially competing to “rule” the world, as some Sci Fi movies use to depict.

Artificial Intelligence will increasingly pervade applications and devices. Few months ago, on June 2024, Sam Altman announced the integration of an Open AI chat GPT based AI assistant on iPhone. This trend will expand soon involving both everyday “tools” and high-end applications and services. Nowadays we talk with our “buddies” *“Hi Google: Set temperature to 24C”*, *“Hello Mercedes play Disco music”* or even closer to science fiction Alexa taking full control of our daily life.

Several services are already managed by artificial intelligence as well as decisions and even critical decisions are assigned to Artificial Intelligence.

AI and ML can offer relevant benefits to humanity, but they must be carefully framed in their potentiality / limits and regulated to avoid potential drawbacks.

AI systems can provide incredible results analysing on the fly billions of data identifying hidden patterns. This can lead to incredible added value outcome in biology, health, text analysis, and more. The main concern expressed by key players in AI field it is not overcoming human intelligence, they are concerned about the potential misuse of such outputs or potential full dependence from AI outputs. AI systems are not “intelligent” as usually assumed by humans, they can provide a valuable output, but they do not “have the intrinsic knowledge or deep understanding” of that output. Thanks to neural networks, even not supervised, they can provide us the best solution, but they do not have the awareness, deep knowledge, of that solution. Close to this aspect we find concerns in the field of AI and ethics.

On May 2024 in Geneve AI for Good general conference and exhibit provided an interesting insight on the state of the art of this set of technologies applied in a wide range of sectors.

One of the most appealing topics was the growing interest in AI regulations, this interest is equally shared between citizens and AI developers.

This set of technologies (AI ML Deep Learning) has generated the need to regulate both the development and the deployment of its applications. Both experts in the field and governmental bodies are asking to issue specific regulations and laws, one of the most relevant voices in this field

was due to Sam Altman “OpenAI’s Sam Altman Urges A.I. Regulation in Senate Hearing” [May 2023] or a newspaper level “The world wants to regulate AI but does not quite know how” [The Economist - Oct 24th, 2023]. Some governments and researchers are asking to add a watermarking on each AI product to be able to easily identify it.

The ‘foul’ use of AI and IoT by hackers can “weaponise” these advanced technologies, terrorists might hack specific IoT devices to ignite thousands of blasts at the same time all-over the globe. In addition, the format of "cyber-crime as a service" is blooming, terrorists have found in cyber-technology the best way both to manage their business and to recruit new "followers".

Recently on the World Economic Forum 2024, Jeremy Jurgens ¹, foresaw the possibility a global cyber-attack that will take us back to the stone age.

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 the already mentioned IoT, 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, in addition the ICCC is every year offering the opportunity to discover new trends and emerging technologies.

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

Three days, official opening ceremony, 29 sessions, Keynote address, several special addresses, two plenary tracks, three parallel tracks, two round table track including a CISO track, 41 cybersecurity

¹ "Geopolitical instability makes a catastrophic cyber event likely in the next two years": WEF Managing Director Jeremy Jurgens on the Global Cybersecurity Outlook Report 2023.

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, Computer Science and 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, a 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 Artificial Intelligence, Ethical, digital transition and more panels.

In addition to the official final statement duly approved by the participants, one of the relevant results 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 and his team, the man who timely understood the relevance of digital transition and cybercrime side-effect 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 will lead to the development of positive and concrete results.