2025 Bucharest Digital Innovation Summit

29 APRIL 2025

Eugen Bulboaca



Reshaping Industries, Threat Models and Institutions

As economies rapidly digitalise, a majority of the new value created over the coming decades will be based on digitally-enabled platform business models. Given the fast adoption rate, staggering competitiveness and free nature of the markets, the private sector is the first to adopt emerging technology, in a never-ending quest of innovation.

Dr. Stephan Schauer, an experienced researcher in the fields of risk management and security at the Centre for Digital Safety & Security located

in the Austrian Institute of Technology (AIT), pointed out that "technological development is a double-edged sword", questioning whether we can determine, without any doubt, if quantum computing is good or not. In practice, development is a requirement and good / bad dichotomy cannot be applied to innovation, given the security implications of not taking any action. Given the fact that technology is in a perpetual development state, its capabilities are growing exponentially, and without active implementation, defence capabilities will quickly be overpowered by those of malicious actors. The essential quality of a tool can only be discerned through the maturity and the trustworthiness of the user. This represents one of the core reasons for the push towards public-private partnerships, especially when it comes to the development of sensitive tools in terms of their abilities.

While technological innovation brings many benefits, including new means of deriving economic value, related risks need to be addressed. These include new forms of cybercrime, data privacy vulnerabilities, and the erosion of institutional trust in both developed and developing economies. The public sector by itself cannot keep up with the pace of progression of these malicious actors, since there is a growing discrepancy in the adoption and development rates between the public and the private sector. Yet, it can lay out the ground in terms of policymaking and initiatives, which would allow private entities to develop efficiently in the name of security. One outstanding example for this is Poland, which sets itself apart through the "Resilience Council(s)" aimed at guiding the digital transformation. These councils consist of experts, which oversee the rapid development of emerging technologies and bridge the divide between the two sectors.

As hazards morph, so must the preparedness. There is a growing necessity for frameworks that strengthen international collaboration through information and technology sharing so that it can address prevention and proportional responses. As such, deep technological understanding becomes crucial at the highest decision-making levels, augmented by expert-led organisational partners.

Strengthening our collective Core Values

There has always been a clash between core values manifesting themselves through ideas, proposals or actions. Traditionally, unfruitful ones were quickly dismissed by a centralised truth-keeping source of information. In contrast, in the digital era, there had been an overflow of unchecked ideas which spread around through the proliferation of social media platforms. Holders of marginal opinions find themselves worldwide support through the ease of international communication, which only strengthens their own conviction. Senior Producer / Foreign Affairs at one of the most prominent Romanian news television channels, Digi24's Cristina Cileacu, suggests that people are starting to lack education, and, critical thinking abilities.

On the Artificial Intelligence front, a growing number of people are starting to rely unquestionably on it. Through the construction of any AI model, there are a number of implicit system decisions, which might propagate some form of unconscious bias. Additionally, since the chain of thought is not explicit, it is even more difficult to verify the origins of the ideas used in the answer composition. The overtrust in AI can have negative effects on populations, beyond lacking accuracy. On this topic, Dr. Christos Kalloniatis stands out as one of the most knowledgeable public figures in the field of "Cultural Technology and Communication". Professor Christos Kalloniatis argues that technology itself is not the problem. Instead, the consumers must present the maturity of discerning good pieces of information from less reliable kinds.

This institutional trust erosion, which can find its origins at the hands of foreign malicious actors, is yet another fight for re-establishing western core values. Coupled with an increase in the number of people that can think critically, misinformation rises as one of the main global risks that beset the western world. In such an environment, awareness, along with institutional collaboration, are key.

Securing Critical Infrastructure

The US Department of Homeland Security defines critical infrastructure as assets and networks – physical or virtual – considered so vital their incapacitation or destruction would have a debilitating effect on national economic security, public health or safety. With this in mind, direct attacks are not necessarily the most destructive in a confrontation. Instead, well-placed attacks on critical infrastructure projects that can cause disruptive chain reactions. With such a great impact, they are continuously under attack from a number of different malicious actors.

Many of these projects are in the hands of the private sector, but the effects of a disruptive attack will spill over to the public. Any breakdown of cybersecurity defences built to protect these functions could result in catastrophe, and the heavy reliance on technology demands a corresponding effort to secure it. To build critical infrastructure resilience, an unclouded assessment of possible threats is required from the moment of inception, as even construction plans in digital format, can pose a later threat to the integrity of the facility. With such high stakes, cybersecurity measures are and should be mandated to all employees of such important projects. After all, security is as strong as its weakest link.

Maritime Critical Infrastructure projects, such as Smart Cables — underwater cables that carry about 95% of the world's internet traffic — present a unique threat. Since these are placed in international waters, it's difficult to traverse the legal regime. Questions as "Who is legally responsible for their protection and responding in case of an attack?" only complicate the matter.

Nevertheless, operational responsiveness plans should be set in place by a coalition of highly competent, well-informed stakeholders.

The Digital Ethos

Technology rapidly has infiltrated into our lives, and migrating to a technology-enhanced life may pose many risks. However, the biggest risk of all is refusing to continue to innovate, to allow ourselves to develop a diluted perspective of unjustified superiority against malicious actors — states or otherwise. With certainty many entities, some of which are hostile, continue to invest in their cyber -attacks and -resilience capabilities. Through public-private collaboration, effective means of communication and general awareness, we will continue to persevere in spite of the challenges we encounter.

EPIS