The Journal of Supercomputing (2018) 74:4865–4866
https://doi.org/10.1007/s11227-018-2614-0

# Threats to critical infrastructure from AI and human intelligence

**Junaid Chaudhry[1] · Al-Sakib Khan Pathan[2] · Mubashir Husain Rehmani[3] · Ali Kashif Bashir[4]**



Without critical infrastructure (CI), the society shall come to a stand still. Today, our life on earth is very much dependent on electricity, global freight of food and goods, telecommunication, healthcare, etc. Except a few human societies living in the forests and remote areas, any community around the globe needs the basic modern facilities. Many industries today, where technology has taken root and made things easier for human workforce increasing their profit margins, are having discussions to replace human workforce with technology—technologies that can offer and use human-like intelligence to mitigate risks and keep processes running, with machine or artificial intelligence. This notion ha s not only created insecurity among human workforce but also has created conundrum for intelligence researchers to develop a product (artificial intelligence) that is derived from discarded (human) intelligence.

Advent of big data analytics, machine learning, and data mining is linked to this "*replacement–movement*" where historical data are used to predict statistical trends along with the confidence factors to make decisions for future. This approach might be sufficiently successful in repetitive, mundane tasks of even *n*th degree of breadth but cannot classify creativity, innovation, out-of-the-box actions, emotional intelligence, etc., which is a classic argument against artificial intelligence in general.

Some might argue against indulging into smart environments where, according to Marc Weiser, "*Technology is so pervasive that if disappears from the forefront*", is not a smart idea after all. We would like to argue against this notion purely in the ground that deeper penetration of technology into our lives is evident and logical; hence, bridges rather than dams need to be built for smoother transition facilitated by more secure and privacy-centric strategies.

✉ Junaid Chaudhry
chaudhry@ieee.org

1 Embry-Riddle Aeronautical University, Prescott, AZ, USA

2 Southeast University, Dhaka, Bangladesh

3 Waterford Institute of Technology, Waterford, Ireland

4 University of the Faroe Islands, Tórshavn, Denmark

Artificial intelligence (AI) is taking over the technology craze at three fronts: 1—data analytics and machine learning, 2—robotics and advancement in actuation technologies, 3—advancement in peripheral technologies, i.e., computer vision, language learning, and context-oriented computing. These three fronts are not too different from the famous push toward AI-enabled technologies of 1980s. Except for now, the technology is far more advanced than what it was before and technology is truly ubiquitous.

The AI is already immersed into our society; example of which is evident when we pull out our smart phone to find the fastest route to city center or use online services to predict when would be the best time to travel to a certain country for holidays, or the like. Indeed, the productivity is going through the roof: thanks to advancements in technology.

Any interruption in technology enabled profit accumulation is deemed threat, a cyber threat. The cyber threats of today come in the shape and forms of astronomical increase in traffic flow to the corporate routers or intrusion attempts to steal data from private servers. Surely, we can mitigate these all-trivial threats using AI. The crux of the matter is that AI is incapable of taking independent decisions, especially the decision where AI is competing with human intelligence (HI). Perhaps, now is the right time to put high stakes in the development of AI and escort the control of the critical infrastructure to AI. Let us give AI a chance to grow and give ourselves an opportunity to contribute to its growth.

If we are to trust AI over HI for numeric superiority in repetitive enumeration and statistical patterns, we will have to invest considerably longer time in developing AI and find harmonious ways where AI and HI coexist in a compatible way. We have special bias toward suitability of self-properties for development of AI. Using self-growing, self-learning algorithms, we shall be able to achieve intellectual superiority in cognitive functions that we are unable to achieve due to physical limitations in HI. Human race, in large masses, depends on integrity of critical infrastructure. As humans, we need to demonstrate the ideal human intelligence paradigm as a model to follow and improve on for artificial intelligence. This effort might create harmony between the two, that is, AI and HI. At this stage, with all its hype, we are far from amalgamating artificial intelligence in our lives let alone in looking after the CI.

In light of the above-mentioned discussion, this effort of ours was to collate the thoughts and latest advancements done by researchers around the globe to tackle cyber threats against critical infrastructure. We had indeed a tough review process through which only few high-quality papers have passed. We hope that the readers will find the accepted set of papers very useful for their future research works.