

The AI – Dual Use Technology?

Anis Bajrektarevic¹

DOI: <https://doi.org/10.60073/euper.2023.4.02>

The international community should rather energetically and urgently work on a new social contract to tackle new technologies and their disruptive potentials. It is particularly related to artificial intelligence (AI) that must be deployed safely and in conformity with a globally shared ethical standard.

Deep fake, dark web, polarising contents, swarms of bots are expanding all over the cyberterritory. Just recall the events that are still shaking western hemisphere: The 2016 US Presidential elections and Brexit vote are still surrounded with a controversy. Their outcome is frequently connected with an alleged leak of personal data from a world's leading social platform to an Analytic agency to reportedly manufacture voters' choices. On the other side, the state (and non-state) actors have deployed huge quantities of motion-tracking and facial-recognition cameras to commodify continuous streams of intimate data about citizens, ostensibly to prepare them for a bonus-malus behavioural grading system.

The bold and commercially promising alliance between the AI and data-ified society has switched most of the contents of our societal exchanges towards the cyberspace. These new masters are already reshaping the very fabric of our realities.

No wonder, our common anxieties are on a rise; Are we losing control to an algorithmic revolution of nanorobots? Is the AI escaping our traditional modes of understanding and collective action? Confidence in our national governance and global stewardship is at breaking point. Popular revolts will follow.

¹ Dr. Anis Bajrektarevic is chairperson and professor in international law and global political studies, Vienna, Austria. He has authored nine books and numerous articles on, mainly, geopolitics energy and technology; he is also editor of the New York based Geopolitics, History and International Relations journal, and editorial board member of several similar specialized magazines on three continents.

Simultaneously, the AI-powered nano-, geo bio- and info- technologies will tend to weaken, rather than to enforce, global and regional governance mechanisms. The UN and similar regional multilateral settings do face a wide range of interconnected challenges. Let us briefly elaborate on some.

THE AI AND DEEPPFAKE

The AI is essentially a dual-use technology. Its mighty implications (either positive or negative) will be increasingly hard to anticipate, frame and restrain, or mitigate and regulate.

The so-called *Deepfake* is a good example. Presently, the advanced algorithmic AI programs have reached the stage to easily alter or even manufacture audio and video images by creating impersonations which are practically identical to its original. Deep-learning facial recognition algorithms can already, with an astonishing accuracy, copy eye-motion, trace and simulate variety of facial expressions or even synthesize speech by analysing breathing patterns in combination with a movement of tongue and lips.

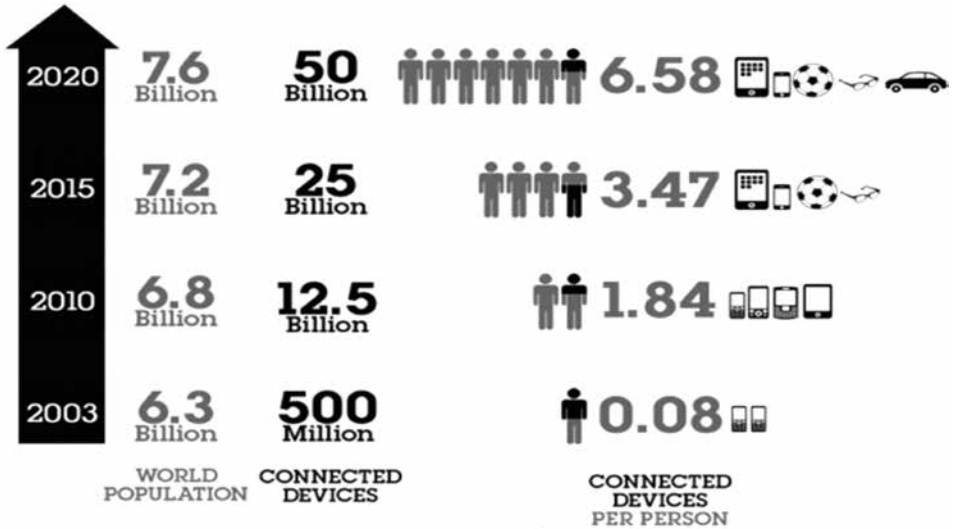
Once released by a state or non-state actor, such artificial interventions could be easily maliciously utilised for a wide range of impacts: political campaigns, racketeering, peer pressures and extortive mobbing. It is not hard to imagine such a fake video triggering public panic (eg. if displays non-existent epidemics or cyberattack), mass demonstrations (eg. if portrays a high-ranking official in bribing scene or similar grave crime), or forged security incidents that may provoke serious international escalations.

The ever-growing number of actors and their increasing capacitation to influence citizens with doctored simulations could pose the long-lasting detrimental implications for the UN and other International FORAs dealing with peace and security. By corroding the very notion of truth and of a mutual confidence between citizenry and their state as well as among states, the *Deepfakes* may turn to be the largest disruptive force to our global governing system.

THE AI AND HUMAN PREDICTABILITY

Due to advancements in the Internet of Things (IoT), the AI is already

bridging and coupling with a range of other technologies, especially with the metadata provided by the Bio-tech. These mergers pose a significant challenge for global security. Driven by the lucrative commercial prospects or by state security considerations, the AI systems around the world are largely programmed towards the predictability of human behaviour. Quite at reach, they already have accurate and speedy analytics of urban traffic patterns, financial markets, consumer behaviour, health records and even our genomes.



These – still unregulated – AI technologies are increasingly able to channel our behavioural and biological data in a quite novel and rather manipulative ways, with implications for all of us. Neither this spares the youngest among us. For instance, the *i-Que* boys’ robot or *Cayla* girls’ doll transmit voice and emotional data of kids interacting with them (of everyone in their 10 meters proximity radius) and send it back to their manufacturers via the Cloud. This feature led the European authorities to examine automated toys closely and conclude that it violates basic principles of consumer and privacy protection. Similar dolls are still in extensive use all over Arab world and Asia where consumer protection awareness is s/lower or less organised than in the EU.

In several OECD countries, the deployment of the court rooms’ emotional analysis is seriously discussed. In such a scenario, the powerful algorithmic biometrics would measure a level of remorse when witnesses are testifying, and audio-video materials are presented. If once

operable, that would be than easily extended by granting corporate (and state) entities to utilise different types of biometrics in assessing the job applicants.

That may furtherly tempt some outcast regimes to force biometric bracelets upon part or even entire populations, and have a real-time and accurate measuring of the popular support they enjoy. (Such bracelets are already heavily advocated in some OECD countries for the prison population, especially for re-convalescent inmates charged with blood delicts.)

Finally, if the humans' individual or group behaviours can be monitored, hoovered, processed and hence, altered, who (or what) will be a driver of electability – be it of a change or status quo preservation – people or algorithms? If the entire biometrics, emotional data and past behaviouristic history (meta) of all parliamentarians, all political parties' protagonists, top military and the key business people is hackable by the national or foreign state or non-state actors – than the sense of democracy, military affairs, security and especially human rights will be changed beyond recognition. Most probably, beyond return, too.

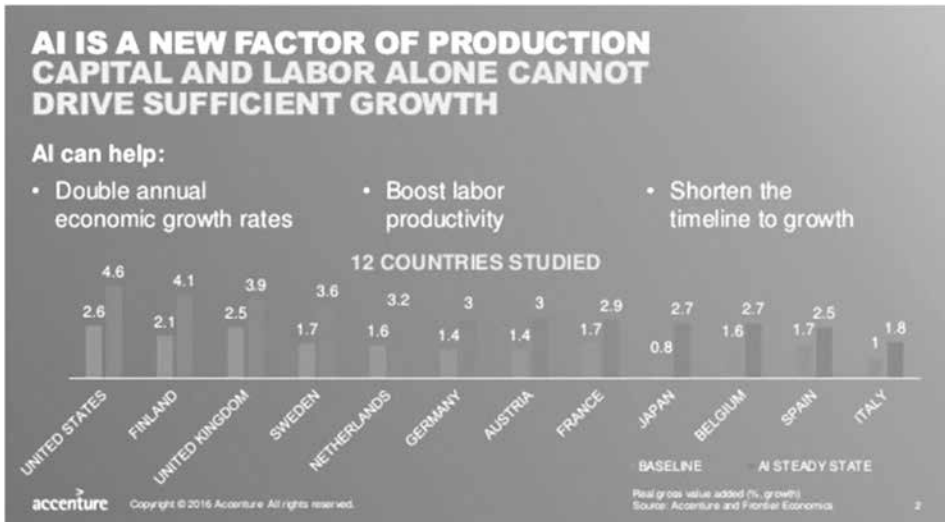
If the AI has such a potential to penetrate – and even steer – individual and group human behaviours, it inevitably disrupts a very notion of human rights as embedded in the UN Human Rights Charter, as well as of peaceful coexistence, security, prosperity and equality among states as stipulated by the UN Charter.

New means of social and biometric control will inevitably necessitate us to revisit and reimage the framework currently in place to monitor and implement the Universal Declaration of Human Rights. Notion of independence and inalienable right to economic development, too. This will require a concerted effort from regional developmental FORAs and the UN as universal multilateral system to anticipate and adjust.

THE AI: THEATRE FOR FUTURE CONFLICTS

Since it reduces jobs in their numbers, configurations and intensities due to automation, the AI is excellently suited for the countries in demographic transition (decline), rather than for the booming demographics of Muslim world, sub-Saharan Africa and of (non-Fareast)

Asia. Dramatic shrinking in domestic labour conjecture and forthcoming shift in global manufacturing dependences will especially hit hard the global south. Often enveloped in the ‘wait-and-see’ stance, the Global south traditionally has a low trust-rate between its citizenry and government.



Logically, the ‘promise of the AI’ to sway large regions and their populations is so immediate and mesmerising, that it already puts its main drivers to a fierce competition. Accelerating competition (with such a disruptive technology) in absence of cooperation (as the best tool to build and maintain confidence) or comprehensive regulation is only one step from a conflict.

The SF-like prospects of ruling ‘AI-race’, thus, are becoming (seemingly) realistic: Powerful state or commercial (technology platforms) actors bitterly competing over our collective data – as a new, cyber currency – to aggregate bio-medical, economic and politico-military supremacy across the globe. The “cyber-colonization” – especially of the global south – is increasingly likely. (Hoovering data without any remuneration and monetising it without any warning, data-collection taxation, or remuneration to its proprietor.) Leaders in the AI field are already capable to globally Hoover data, are in possession of storing capacities, and will soon master (quantum) computing powers to process and analyse, and potentially control other countries’ populations and ecosystems.

THE ANSWER TO AI SHOULD BE UNIVERSAL

Quite disturbingly, our societies are far from prepared for deployment of the AI: Be it philosophically or practically, we are still short of a thorough socio-political, legal or ethical considerations. Moreover, the UN and its Agencies – architected 75 years before the emergence of these technologies – are in many aspects poorly equipped to offer comprehensive and timely AI governance. Speed of this technological innovation cycle outpaces any administrative response, even as the technological disruptions are becoming apparent to ever larger number of countries. In the near future, they will increasingly come in unpredictable severities and frequencies, and in hard-to-connect contexts.

The new political trends of autarchic ‘neo-nationalism’ are further trivializing capacity of the multilateral FORAs to play a norm-setting and monitoring-of-compliance role in the global governance of AI. In such a climate, technologically advanced Member States (pressured by their national security or commercial interests) may see little incentive in letting the international FORAs to govern what they perceive as own lucrative and proprietary technology. Thus, collective decision-making mechanisms could sink into the dark of obscure centres of projected power, out of reach or any control.



Having all this in mind, the UN and its Specialised Agencies (including the ITU, UNESCO and UN University), along with variety of regional FORAs hold the answer. That very much includes the developmental segments – especially of global South – such as the African, Asian, Interamerican or Islamic Development Banks as well as regional politico-administrative settings like the OIC, SAARC, ASEAN, AU, to name but few. They have to initiate and navigate their member states, but also participate in steering the world through the universal, UN bodies.

Letting the AI train to pass without a collective, collaborative form of governance would be a double irreversible setback: Disruptive dual-use technology along with a digital ownership would be handed over to an alienated few to govern it, while the trust in multilateral system (especially within the developing world) would further deteriorate.

Such inaction would inevitably raise the level of planetary confrontation to unfathomable proportions (including new forms, unseen so far), and that on two fronts – within societies and between states. Some would do anything to dominate and rule, while others would do anything to escape the iron fist of goo(g)lag.

For the three gravest planetary challenges (technology, ecology, nuclear annihilation), we need an accurate just and timely multilateral approach. In this struggle for relevance, everyone has its own share of historical (generational) responsibility.

POST SCRIPTUM

Back in 2011 (while feeling the amplitude but not yet seeing the today's dimensions of its omnipresence and pervasiveness), I coined term a *McFB* way of life. Then and there – in my book 'Is there Life After Fb', I noted:

Ergo, the final *McSociety* product is a highly efficient, predictable, computed, standardized, typified, instant, unison, routinized, addictive, imitative and controlled environment which is – paradoxically enough – mystified through the worshiping glorification (of scale). Subjects of such a society are fetishising the system and trivializing their own contents – smooth and nearly unnoticed trade-off. When aided by the IT in a mass, unselectively frequent and severe use with-

in the scenery of huge shopping malls² (enveloped by a consumerist fever and spiced up by an ever larger cyber-neurosis, disillusional and psychosomatic disorders, and functional illiteracy of misinformed, undereducated, cyber-autistic and egotistic under-aged and hardly-matured individuals – all caused by the constant (in)flow of clusters of addictive alerts on diver-ting banalities), it is an environment which epitomizes what I coined as the *McFB way of life*.

This is a *cyber-iron cage* habitat: a shiny but directional and instrumented, egotistic and autistic, cold and brutal place; incapable of vision, empathy, initiative or action. It only accelerates our disconnection with a selfhood and the rest. If and while so, is there any difference between Gulag and *Goo(g)lag* – as both being prisons of free mind? Contrary to the established rhetoric; courage, solidarity, vision and initiative were far more monitored, restricted, stigmatized and prosecuted than enhanced, supported and promoted throughout the human history – as they've been traditionally perceived like a threat to the inaugurated order, a challenge to the functioning status quo, defiant to the dogmatic conscripts of admitted, permissible, advertised, routinized, recognized and prescribed social conduct.

Elaborating on a well-known argument of 'defensive modernization' of Fukuyama, it is to state that throughout the entire human history a technological drive was aimed to satisfy the security (and control) objective; and it was rarely (if at all) driven by a desire to (enlarge the variable and to) ease human existence or to enhance human emancipation and liberation of societies at large. Thus, unless operationalized by the system, both intellectualism (human autonomy, mastery and purpose), and technological breakthroughs were traditionally felt and perceived as a threat.

Consequently, all cyber-social networks and related search engines are far away from what they are portrayed to be: a decentralized but unified intelligence, attracted by gravity of quality rather than navigated by force of a specific locality. In fact, they primarily serve the predictability, efficiency, calculability and control purpose, and only then

2 Shopping malls – these vertically erected symbols of our horizontalities – are increasingly occupying urbanistic and social centrality of our civilizational contents. These air-conditioned parameters are gradually substituting the traditional axes of urban sociableness (such as sacral edifices, theaters, galleries, operas, public parks, sports halls and the like). Attended persistently and passionately, they are emerging as new temples for the XXI century believers, who worship the polytheistic gods of free market (with mobile gadgets in uplifted hands, instead of sacral candles, illuminating their faithful faces). The functional focality of shopping malls nowadays is steadily transforming a large spectrum of socio-cultural possibilities into a box of addictive consumerist probabilities.

they serve everything else – as to be e.g. user-friendly and *en mass* service attractive. To observe the new corrosive dynamics of social phenomenology between manipulative fetishisation (probability) and self-trivialization (possibility), the cyber-social platforms – these dustbins of human empathy in the muddy suburbs of consciousness – are particularly interesting.