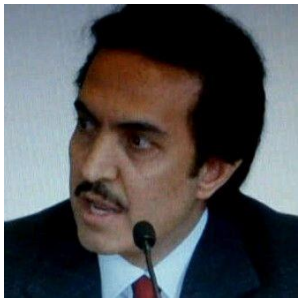
OXFORD POLITICAL REVIEW

Major Transformative Technologies and the Five Dimensions of Security



Nayef Al-Rodhan June 23, 2020

Cyberattacks and data theft have received a rating between 3.5 and 4 out of 5 in the 2020 World Economic Forum Global Risks report. Our societies' ubiquitous reliance on technologies naturally comes with downsides.

It is now commonplace to refer to new technologies as transformative forces in the 21st century – with the attendant discussions of opportunities and risks. In this article, I want to provide an overview of five transformative technologies poised to impact global security in a holistic sense.This paper provides a succinct presentation of these technologies, as well as – it is hoped – a clear and structured overview for policymakers and concerned citizens to understand their long- and short-term implications for security.

The types of technologies presented in this article are interlinked and create systemic vulnerabilities. The first technological field discussed here is related to data itself, *Big Data*, and subsequent technologies cover systems using extensive data sets: *AI & Machine Learning, Quantum Computing, Neuromorphic Computing.* One field in life sciencesappears particularly powerful and with far-reaching implication for global security: *Synthetic Biology*.

I provide a survey of the security risks of these technological fields using my multi-sum security paradigm, which introduces my classification of the five dimensions of security: *human, environmental, national, transnational* and*transcultural*. This allows for a more comprehensive approach to security and is especially relevant in evaluating the multi-faceted risks triggered by disruptive technologies.

Big Data

'Big Data is used to describe the massive volume of both structured and unstructured data that is so large it is difficult to process using traditional techniques.' Big Data impacts all aspects of our lives from health and resources to communication and is fundamental in the training of machine learning systems.

Big data triggers *human security* risks by endangering individuals' privacy and civil liberties. Overreliance on Big Data in policing and in judicial processes has also demonstrably led to overly harsh punishments and unfair treatment. This reinforces feelings of fear, vulnerability and mistrust in institutions, and can be detrimental to social cooperation and the social contract.

Environmental security can be enhanced in multiple ways by Big Data (e.g. through better predictability and more accurate data on air pollution for climate researchers) but it simultaneously introduces risks mainly related to the energy consumption required for management and storage. For example, 'US data centers use more than 90 billion kilowatt-hours of electricity a year, requiring roughly 34 giant (500-megawatt) coal-powered plants', and this consumption could 'double every four years'.

In terms of *national security*, the theft of strategic information is an important challenge. For instance, in May 2020, during the Covid-19 pandemic, the United States claimed Chinese hackers tried to steal sensitive data concerning research on treatments and vaccines against the virus.

These behaviours weaken *transnational security* by feeding a race for data and compromising governmental information. Criminal networks, operating transnationally, can also increasingly leverage the so-called 'cloud' technologies for their illegal profits.

At the *transcultural security* level, there are clear biases in data collection and analysis. Current data mining relies mostly on inputs from privileged communities where internet penetration is high and are not representative of various cultural norms. If critical infrastructures become increasingly reliant on these records, the result will be structural and inbuilt discriminatory systems, which will be difficult to overcome.

Artificial Intelligence & Machine Learning

Artificial intelligence (AI) is commonly understood as '*the theory and development of computer systemsable to perform tasks normally requiring human intelligence*.' Machine learning (ML) is a sub-field of AI relying on datasets fed into a system that learns from it. The machine 'starts to understand the behaviors and what things look like and what they do instead of what they are.'

One way in which AI endangers *human security* is through the introduction of greater labor-market instabilities. According to Oxford Economics, 20 million manufacturing jobs could be lost by 2030. Another critical risk involves mis-profiling and the wrong inclusion into AI-generated watch lists, inevitably resulting in aggravated vulnerability for certain social groups. Additionally, *human security* was defined by a United Nations resolution as 'the right of people to live in freedom and dignity, free from poverty and despair.' With ML development, individuals – at least in some economic sectors – might be surpassed by machines. In line with our inherent *emotional amoral and egoistic* nature, questions of self-esteem and considerations for human competencies could endanger self-worth and agency.

There are notable aspects of *environmental security* where AI systems can have a negative effect, and one of this is the reliance of AI on Rare Earth Elements (RREs). In China, which dominates the world supply of RREs, providing 97% of the world output of rare earths, the chemicals discharged to process these minerals damage soils, water, and ecosystems. Furthermore, numerous agricultural and water systems rely on AI technology. As an example, Microsoft developed AI tools to enhance agricultural processes through land monitoring. If corrupted data is transmitted, consequences could be significant for ecosystems and food supplies. In the oil and gas industry, which is now also reliant – at least to some extent – on machine-learning, detection and extraction processes are improved by analyzing seismic data quickly. The result is that this may create a surge in drilling worldwide.

AI introduces numerous risks for *national security*. Unmanned Aerial Vehicles (UAVs) for surveillance and combat operations have been providing precise images, videos and spatial information, but errors in the system could endanger civilians and critical infrastructures. ML also brings new tools, such as deep fakes, in the field of information warfare. They allow for the artificial reproduction of videos and images from elected officials and other public figures, which can compromise electoral processes.

One of the *transnational security* risks associated with AI is the vulnerability it introduces for global digital systems such as financial flows. AI could notably become an accelerator of financial criminality through faster systemic implementation of malware and automated data theft. In ML,

systems could be flooded with adversarial examples which could cause serious damage to citizens and infrastructures. The lack of transparency generated by these tools could also diminish the prospect of any international legal instrument to regulate these practices.

At the *transcultural* level, biases contained in data sets could create discriminatory machine systems. Such standardization could create further tensions notably with minorities. Additionally, AI can uncover deep ethical conflicts. ML systems could be trained to a point where they also extract the worst of our emotional behaviors and replicate it. We could imagine this to occur in various contexts and institutional settings, including in multilateral fora, such as the Group of Governmental Experts (GGE) on Lethal Autonomous Weapon Systems (LAWS), which reached a deadlock in August 2019 over notions of human control. The contentions can be understood as reflecting different cultural attachments to human judgement and agency.

Quantum Computing

Quantum computing is a type of computing power that harnesses the potential of quantum mechanics, a very complex, "almost-mystical" set of phenomena using subatomic particles properties such as *superposition* (two states added together to create a different state) and *entanglement* (occurring when particles are generated, interact or are close so that the state of each particle cannot be described independently of the state of others). Unlike conventional computing devices, quantum computers do not use binary code, but rely on quantum bits, and have an extraordinary computing capacity, as well as – to date – un-hackable encryption. Once fully developed, quantum computers could supersede the fastest and most powerful supercomputers, and according to some scientists, they could also accelerate artificial intelligence. Quantum computers promise to revolutionize many fields, from pharmaceuticals to material science and outer space. But, as always, embedded in opportunities are also the risks.

One way in which these technologies could endanger *human security* is through the violation of individuals' privacy. Quantum computers could potentially unlock all current mainstream systems of encryption and passwords security such as Transport Layer Security (TLS) or Advanced Encryption Standard (AES).

In terms of *environmental* security, a significant issue concerns the refrigeration required for quantum computers, which necessitate significant power and resources. Going forward, it will be critical to resolve this challenge, to ensure that the hoped-for benefits of quantum computers for combatting climate change are not offset by the environmental costs of the quantum computers themselves.

National security risks include encryption breaks which could endanger sensitive information, critical infrastructures, diplomacy and control of weapon systems. At the same time, states could gain an information advantage which would enhance their ability to influence other states and international entities.

At the *transnational* level, the use of satellites to ensure quantum level encryption in communication, could make space assets a valuable target, including by non-state actors. Interesting to note, however, that Raytheon Company has already developed a satellite defense system based on quantum properties.

In terms of *transcultural security*, quantum computing could deepen differences in uncertainty avoidance due to their unpredictable future. Indeed, according to the cross-cultural sociologist Geert Hofstede, cultures react differently to ambiguity, uncertainty and risk. Some societies might accept this unknown while others may meet it with more resistance.

Neuromorphic computing

Neuromorphic technology is a recent and fast-developing field that is premised on replicating the neural architecture of the brain. Neuromorphic computers do not operate in a linear fashion but mimic the architecture of the brain, with millions of interconnections between neurons, high efficiency and robust learning. One of the most advanced and best-known projects in the field is the TrueNorth chip created at the IBM, which developed a neurosynaptic core that integrates both computation and memory (unlike the 'von Neumann architecture') and does not have one large processing unit, but many artificial neurons which are interconnected. IBM's brain-inspired computer was originally designed with 4,096 processing cores, mimicking one million human neurons and 256 million synapses. In initial tests, the computer was already able to complete some common AI tasks, such as recognizing images – yet much faster and using less power. Other areas of research also built upon knowledge from recent years about the link between paradigms of reinforcement learning in machine learning and reinforcement learning in the brain; similarly, it was shown that neuromorphic computation can work with a spiking neural network which learns to solve a task smoothly via the mechanism of reinforcement learning.

Neuromorphic computers could bring opportunities in varied fields, from medicine, to data mining, and national security, military equipment (e.g. highly intelligent drones). However, as always, risks underscore these developments too.

In the area of *human security*, neuromorphic chips integrated into robots would be able to grasp the world as humans. In a worst-case scenario, they could develop the worst of our attributes such as selfishness and threaten other human beings. Novel generations of robots, including robots with moral competencies, would pose a significant risk to the social order, and to our existing systems of laws and rights. In such a future, the idea of robot rights, and granting robots due recognition and personhood, may be unavoidable.

Neuromorphic computers also present risks for *environmental security*. The production of silicon computer chips for conventional computers already comes with a significant environmental cost using gases, water and various chemicals. Neuromorphic chips, which are composed of brain-like neurons and synapses made of silicon, require silica mining, which may be increased, with significant environmental and health costs.

In terms of *national security*, neuromorphic technology could bring national surveillance to a whole new level with sensors replicating human eyes, making object and face recognition more effective. The technology could also improve the capability of existing drone and systems of recognition used in warfare – and create a new domain of competition between states.

In a similar vein, *transnational security* would be impacted by neuromorphic computers introducing new drones and robots with brain-like chips, making spying much more effective. The risks raised for *transcultural security* echo the ethical and existential risks mentioned above: the possibility for robots to build their own moral code is certain to be contentious even in the most secular contexts.

Synthetic Biology

Synthetic biology is defined as the 'the application of science, technology and engineering to facilitate and accelerate the design, manufacture and/or modification of genetic materials in living organisms.' This technology promises to benefits climate research, enable remedies for environmental degradation, or in agriculture, plant circuits and crops. At the same time, synthetic biology introduces significant challenges for national and global security – one notable risk highlighted in

recent years refers to the possibility of non-state actors engineering deadly pathogens, but the challenges synthetic biology extend further.

One important risk for *human security* is the impact on our fundamental right to health and the privacy of our biological and genetic data. Biological threats could be increased by the mis-manipulation of pathogens in laboratories.

These threats can extend to *environmental security*, as artificial pathogens created in laboratories could damage land or water supplies. The rise of 'Do-It-Yourself Biology' further augments this risk as it becomes simpler to develop a makeshift lab without strict supervision.

New bio-weapons created from harmful synthetic organisms – though still not easy to assemble – will pose a unique kind of challenge to national security, making medical responses very difficult especially in cases of harmful new pathogens. Additionally, such risks may come both from states and non-state actors, thus multiplying the sources of threat. These risks manifest in the area of *transnational security* as well, as biological warfare and biological terrorism can gain new momentum.

With regards to *transcultural security*, synthetic biology could prompt or enhance clashes in societal and cultural values. Reactions to previous innovations in life sciences could be an indicator. For example, monotheistic religions' official position was to authorize genetically modified food but some groups remain firmly opposed to this practice. In a similar way, strong opposition could rise against synthetic biology and any attempt to modify genetic materials in living organisms.

Social Contract 2.0 and going forward

This brief overview of risks associated with these select list of transformative technologies shows their far-reaching implications for global security.

Approaching these systemic risks requires a holistic approach, one that will allow for the protection of our nine dignity needs: *reason, security, human rights, accountability, transparency, justice, opportunity, innovation* and*inclusiveness*. Without the appropriate oversight and tight regulatory processes that set limits on the permissible features of these technologies, they will end up creating more conflict and tensions nationally and globally.

To tackle the surveillance capabilities amplified by new technologies, I previously suggested moving towards a 'social contract 2.0': the imperative to enhance constitutional guarantees and the protection of freedoms, rights and human dignity in the context of this ubiquitous and intrusive digital revolution. The new technological possibilities we are faced with today, however, bring risks beyond surveillance and social alienation, and beyond the ability of states to handle alone. To meet these risks, states must exercise more vigilance in the development of new technologies. While approaches to regulation may vary from industry to industry, regulation must abide by some commonly agreed methodologies and standards of risks –includingexistential risks. In dealing with private tech companies, one approach that is increasingly encouraged is *self-regulation*, which means thattech companies setethical guidelines on the research and development of technologies.

This approach has been shown to work especially well in sectors where companies are confronted with significant competition. States should commit to collaborating with, or purchasing products from companies that exercise stringent calculations of risks. However, this approach has obvious limitations (of trust and accountability), and going forward, and especially as governments will need to regulate more invasive and dangerous technologies, the role of independent and parliamentary ethical commissions could be essential. This has already been done in some sectors (one recent example in

the UK is the 2019 Inquiry on Immersive and Addictive technologies) and it must be promoted as a critical instrument for the regulation of technologies in the future.

In using these intrusive technologies, the goal for states must be to balance the "need to know" and to keep populations safe and secure, with safeguarding privacy, dignity and civil liberties for all. States must also have a system of "overseeing the overseers" to insure transparency and accountability, and to make sure that the surveillance data of populations is guarded against leakage to private actors, and against potential misuse and abuse.

In addition, parliamentary and expert inquiry boards must be multidisciplinary in order to reflect the full implications of these technologies for the economy, for social cooperation, and for future of humanity. The inevitable impact of some of these technologies on humanity, largely speaking, means that states must also increasingly support bringing these topics to international and multilateral settings, where creative exchanges and regulatory frameworks can advance solutions to minimize risks without stifling innovations.

Prof. Nayef Al-Rodhan (@SustainHistory) is a Neuroscientist, Philosopher and Geostrategist. He is an Honorary Fellow at St Antony's College, University of Oxford, and Senior Fellow and Head of the Geopolitics and Global Futures Programme at the Geneva Centre for Security Policy, Geneva, Switzerland. Through many innovative books and articles, he has made significant conceptual contributions to the application of the field of neurophilosophy to human nature, history, contemporary geopolitics, international relations, cultural studies, future studies, and war and peace.