# Why agile governance should be human-centred governance

14 Sep 2020

Nayef Al-Rodhan

Honorary Fellow, St. Antony's College, Oxford University

Boxes of genetically modified mosquitoes are displayed to the Brazilian media before release. Such use of gene-editing calls for agile regulation.

Image: Reuters/Paulo Whitaker

It is no secret that COVID-19 has exacerbated the need for quick decision-making, rapid development and the broad implementation of technology. This period of accelerated technological advancement runs parallel with the release of updated regulatory guidance for the Fourth Industrial Revolution from major governing bodies such as the EU, the US and China. The arrival of a pandemic has shown that the two do not necessarily correlate and begs the need for stronger principles of agility in governing technology.

On the one hand, there are concerns about stifling innovation, and therefore the need to limit regulatory "overreach", as the US approach demonstrated in its 10 principles for government agencies for regulating the private sector. On the other hand, there are ethical concerns for the levels

of safety, trust and discrimination that machine-learning and big data can overlook if not properly regulated, as targeted in the EU's White Paper in February.

The question is: How do we mitigate the adverse consequences of disruptive technologies and maximize sustainability and inclusivity, while keeping pace with the industry? And why must these frameworks be, above all, human-centred? I have previously argued that security is not just about "national security", but has five dimensions that must be addressed: Human, National, Environmental, Transnational and Transcultural Security. Taking all of them into account, many aspects of agile governance might be said to converge towards what I have previously called "dignity-based governance".

**1. Human security**

Human security is fundamental to policy-making. How secure we feel about our privacy, data, competencies and self-worth all feed into the vulnerabilities exposed by emerging technologies. Our emotional, amoral and egoistic nature means that any detected mistrust or violation of our dignity can lead to non-cooperative attributes of our nature, such as fear and pre-emptive aggression.

The issue of trust has been heightened over the course of the pandemic. We want to trust our governments throughout the world to do the right thing – we trust our governments to save lives. However, this is a layered process.

Last month, the UK government conceded that its test and trace system, designed to track contacts of people infected with COVID-19 through the provision of personal details, had been launched without following its own Data Protection Act 2018.

If governments are to prioritize human dignity in their governance frameworks, they must respond to our critical nine dignity needs: reason, security, human rights, accountability, transparency, justice, opportunity, innovation and inclusiveness. This will allow for maximum adaptability and sustainability in governance systems.

**2. National security**

As the commodification of information increasingly entails digital risk, our human security is also dependent on robust national security.

In Estonia, data storage is decentralized: Government and private sector institutions have their own servers, which are centrally connected. It also makes it more difficult to hack Estonia's data, and ensures that citizens have control over which government body or private entity can access their personal data. This is vital to secure privacy control and accountability in the use of public data to build a culture of trust that is ultimately sustainable.

However, the harsh reality of our disparate socioeconomic landscapes mean that data access is not available to the same extent for the whole population. Factors such as lower rates of smartphone and computer ownership in economically disadvantaged and elderly groups must be taken into account as we work towards frameworks where all are able to have a secure hold of their data.

**3. Environmental security**

The environment and our natural resources also have a role to play across the peace and security continuum. As we deepen our understanding of the stresses linked to climate change, water and food insecurity, we have been forced to revise our approach to the impact of emerging technologies on environmental degradation and its consequences for human security.

The disruptive environmental impact technology can have on labour markets is also better understood now than during previous industrial revolutions, allowing for more agile solutions.

Smart Information Systems (SIS) provide farmers with local weather predictions, farm efficiency and sustainability metrics. As the UN has projected the global population to swell to 9.8 billion by 2050, forcing the agricultural sector to increase its production levels by up to 70%, SIS are being hailed as a possible solution to help to harvest and manage farms more effectively. However, agile regulation must allow room for ensuring the reliability of data and the protection of the farmer's data ownership to ensure the principles of inclusivity are met.

Though it has been widely praised, synthetic biology – especially, an innovative form of gene-editing, CRISPR – also raises ethical and sustainability issues. The challenge of agility largely lies in the unpredictability of the science, as well as the interconnectedness of cross-sector cooperation.

For example, the dissemination of gene-edited mosquitoes, designed to combat malaria and other illnesses, could have unintended consequences outside of the small, confined spaces of a lab, and among other species of the same organism. For example, in some cases mosquito populations have inadvertently been amplified rather than reduced. This is because scientists are still working out how various species fit into the complex ecosystem, and many of these scientists are working in countries that are not directly affected by the diseases in question.

The WHO is currently in the process of designing an agile framework to meet these environmental challenges. In January of this year, it released its draft governance framework for human genome editing, underlining transparent, inclusive, responsible collaboration as its key message to governments and stakeholders.

**4. Transnational security**

In order to meet the challenges of the above, a cooperative global regime for agile technological governance is vital. Much of the narrative around the US and China as leading global players in the field of emerging technologies, focuses on a potential AI "arms race" as each tries to assert its authority in the field. In this respect, their overarching focus on dominance in the industry neglects the human element as a central priority.

However, Jeffrey Ding, from the University of Oxford's Future of Humanity Institute, suggests that the US and Chinese AI ecosystems are still very much entwined. The reality is that states are not involved in a zero-sum game, as political rhetoric may suggest, but rather they are symbiotically connected and interdependent.

Whether states like it or not, transnational threats such as disruptive technologies mean that the actions – or inaction – of people and governments anywhere in the world can harm others. Governments are thus unable to effectively address these issues unilaterally and instead must work with private and state partners, using agile principles to bridge any differences to collaborate in a way that coherently addresses the challenges they face.

**5. Transcultural security**

International governments must also be aware of the global historical and cultural context in order to avoid situations of marginalization and prejudice that destabilize any chance of a sustainable, inclusive and secure governance framework.

Countries and private firms that can leverage AI to industrialize innovation stand to have a degree of political, economic and military power, whereas existing multilateral institutions often lack the capacity to maintain the same pace, not to mention countries that have been historically ostracized.

That being said, the US's five-decade reign of the internet-driven era is shifting from a unipolar technological hegemony to a landscape where countries such as China, Brazil and Russia are becoming increasingly competitive and re-writing the rules of their own digital trade agreements.

A global agile governance framework would endeavour to recognize contributions from each and every culture and grant respect and due recognition to each. We need more accountable guidelines and assessments of AI around fairness, trust, bias and ethics to ensure that governance agility, sustainability and inclusion form the basis of regulation with human dignity at its core.

**The ideal model**

Any sustainable and agile governance model must balance the ever-present tension between an emotional, amoral and egoistic human nature and its corresponding nine dignity needs: reason, security, human rights, accountability, transparency, justice, opportunity, innovation and inclusiveness.

This will improve cooperation, reduce conflict, enhance domestic and global prosperity while maximizing the chances of sustainable global security and a more stable global order.

It will also ensure that governments will be more resilient and secure, thus accentuating the possibilities of cooperation and collaboration on innovative new methods such as those surrounding regulation on the Fourth Industrial Revolution.

**Written by**

Nayef Al-Rodhan, Honorary Fellow, St. Antony's College, Oxford University