



# Metis

## Study

### **Great powers and digitisation: What are the implications for world order?**

No. 08 | October 2018

The views expressed in Metis Studies are those of the authors. They do not reflect the opinion of the Bundeswehr, the Federal Ministry of Defence, or the Bundeswehr University Munich. The primary target audience of Metis Studies are practitioners. Metis Studies are based on analyses of scholarly literature, reports, press articles and expert interviews with academics, think tank analysts and policy-makers. References are omitted. Inquiries about sources can be directed at the author(s) via email.

# Summary

**T**his study focuses on the triad of data, its processing and its conversion into economic and military power to shed light on the race between the United States and China for supremacy in the digital age. It highlights arms and arms control,

strategic stability and, prospectively, the implications of a potential quantum computing revolution. The study ends with a number of further-reaching thoughts regarding the implications of the digital age's world order for liberal democracies such as Germany.

## Data, artificial intelligence and power

Data is the oil of the 21st century. This popular analogy may be flawed, but it draws attention to a connection that is decisive for this study: Data – the capabilities and possibilities of collecting it, the capacities for processing it by means of artificial intelligence (AI)<sup>1</sup> and thus the opening for converting it into economic and military power – will be of crucial importance to the world order in the age of digitisation. Civilian technology companies are the driving forces behind innovation. Private investments exceed those of the public sector and the military many times over.

In the US, the Pentagon seeks closer ties to technology companies in Silicon Valley. Strategically speaking, Washington has switched from the war on terror to great power conflict. Military use of AI technologies is meant to retain its own conventional superiority (Third Offset Strategy).

China stated in 2017 that its official goal was to achieve global leadership in AI innovation by 2030. Beijing is working on civil-military integration as well. The country intends to also make military use of the results of its

breathtakingly fast race to catch up commercially (“intelligensitisation” of warfare).<sup>2</sup>

This study examines the implications of the digital age for great power politics in three militarily relevant areas, taking China and the US as examples. The analysis spotlights arms and arms control, strategic stability and, looking ahead, the use of quantum computers. The focus is widened in the conclusion. It addresses the future of the liberal democratic model of society in the world order of the digital age.

## Arms and arms control

The USA and China are both striving to transfer digital innovations from the civilian sector to military applications. They face two challenges. The first is the diffusion susceptibility of digital technologies (due to this, monopolies are much harder to maintain than with previous military high technologies such as stealth). The second is the incompatibility of military procurement processes and requirements with short development cycles of commercial products and solutions that are also sometimes unreliable.

With its Defense Innovation Unit Experimental (DIUx) branch in Silicon Valley, the Pentagon has been responding to these challenges since 2015 by seeking greater proximity to civilian technology companies. However,

---

<sup>1</sup> The broad and inconsistently defined concept of artificial intelligence encompasses a variety of software-based techniques and processes for automating specific tasks that have previously required the use of human intelligence.

---

<sup>2</sup> For China, the victory achieved by the AlphaGo software (developed by Google DeepMind) over Go champion Lee Sedol in 2016 was a “Sputnik moment”.

the deliberate attempt by the US military to tap into the US commercial sector is not undisputed, as the Maven pilot project showed exemplarily. This cooperation project between Google and the Pentagon was a software infrastructure based on machine learning designed to recognise objects and persons in drone footage automatically and so be able to take over some of the more tedious work of human analysts. After it became known, the pilot project was met with massive resistance from Google employees who rejected it as heralding algorithmised, dehumanised warfare. In June 2018, the Google management felt forced to declare that it would not renew its Maven contract with the Pentagon after its expiration in March 2019. In the AI principles subsequently developed and published by the corporation, it restricted cooperation with the military and (almost)<sup>3</sup> completely refused to work on weapon systems. Moreover, Google withdrew from the bidding competition for the Joint Enterprise Defense Infrastructure (JEDI) project valued at around USD 10 billion and intended to help the Pentagon create a military cloud. Google's competitors initially seemed unimpressed, but tech workers at Amazon and Microsoft have recently also mounted organised resistance against the JEDI project.

Nothing similar is known to take place in China. This is in no small part due to secrecy and a lack of transparency on account of the semi-permeable language barrier. This latter factor enables Chinese tech experts – a large number of whom have been trained abroad and have a command of English – to follow English research and innovation while there is hardly any information exchange and knowledge transfer in the opposite direction. Open sources do not provide sufficient information to speculate as to whether the Chinese military is like the Pentagon in that it maintains cooperative relations with Alibaba, Baidu or Tencent and whether there are similar concerns or objections to those voiced in the USA. Translations of official Chinese debates and documents (especially the White Paper on Civil-Military Fusion and AI) suggest that intensive efforts are in fact being made. But unlike in the West, where – beyond the US examples of Maven and JEDI – civil society and experts generally call military use of AI techniques into question, gathering considerable media

attention,<sup>4</sup> we know of only one renowned AI researcher in China who has publicly taken a similarly critical stance.<sup>5</sup>

The growing importance of data and software in the military sector also means completely new challenges for arms control (among great powers). The quantitative paradigm of the 20th century is only valid to a limited extent. Numerical limits and counting rules have up to now been the key elements of both nuclear and conventional arms control. Negotiators in the nuclear field have counted warheads and delivery systems, those in the conventional arms field have measured lengths, heights, widths and weights. This approach is less relevant for conventional high technology that increasingly relies on software, and it is of no significance at all for cyber capabilities. When the effectiveness of a physical weapon system primarily results from externally invisible factors such as the degree of autonomy or interaction with distributed sensors and other weapon platforms, it is much more difficult to verify arms control agreements.

A qualitative paradigm will have to be added to the quantitative one in the digital age for arms control to retain its function of helping to ensure political stability. Whilst this realisation is not new and has long since been discussed among arms control experts, research into solutions has only just begun. One thing, however, is certain: digital technologies are not only a challenge for arms control, but also an opportunity. For example, initial studies into the use of distributed ledger solutions (blockchain) in the nuclear non-proliferation regime suggest that new horizons open up for both arms and arms control in the digital age.

### Strategic stability

The opportunity to automate processes is a key feature of the digital age – in both the civilian and the military sector.<sup>6</sup> In the highly sensitive and notoriously conservative nuclear field, process automation has unique limits. Decision-making on the use of nuclear weapons will not be automated (in the foreseeable future). All the nuclear powers will (hopefully) clearly remember the case of Lieutenant Colonel Stanislav Petrov, the officer in charge who, in 1983, doubted the alert issued by the Soviet early-warning system that reported a US nuclear attack and thus

---

<sup>3</sup> The Google AI principles suggest that – after weighing up all the relevant aspects – the company might make an exception for weapon systems that solely engage objects. A plausible example would be defence systems that are only directed against ammunition.

---

<sup>4</sup> Examples include the open Future of Life Institute letters, which are signed by many leading researchers in AI and related fields as well as prominent intellectuals. They include Demis Hassabis and Mustafa Suleyman from Google DeepMind, the late Stephen Hawking, and Elon Musk.

<sup>5</sup> Prof. Zhou Zhihua from Nanjing University.

<sup>6</sup> In the latter, this may go as far as selecting and engaging targets without human control, see “The security-policy effects of digitisation”, Metis Study No. 1 (February 2018).

prevented a likely nuclear escalation. Petrov later justified his – correct – decision by pointing out that the warning system was new, that the number of reported US missiles was too small to make sense as a first strike and that his overall gut instinct caused him to doubt the validity of the alert. The example of Petrov shows that human judgement relies on the capability to interpret numerous subtle pieces of contextual information. Similar decision-making powers will not be mechanically reproducible in the foreseeable future.

There is no greater probability of existential decisions on the use of nuclear weapons being delegated to algorithms than there is of strategic stability being endangered by direct accesses via the Internet.

Nevertheless, the Internet and the digital age increase certain risks inherent in the nuclear enterprise,<sup>7</sup> especially those of miscalculation and misperception. Such indirect risks include manipulations of the information landscape in which politico-military decisions are made. Much attention has recently been attracted by the deep fake technology that is based on deep learning, especially deep fake videos that can be produced and disseminated in real time for manipulative purposes. In an age in which the US president uses Twitter as his primary communication channel and North Korea is a nuclear power, new manipulation and escalation scenarios become real.<sup>8</sup> Familiar risk-reducing measures such as no-first-use doctrines or the lowering of the nuclear alert status to buy time in crisis situations thus gain renewed relevance for arms control.

### Quantum computers: The next revolution?

The transmission belt used to convert data into economic and military power is currently constituted by the increase in the computing capacity of conventional computers in combination with machine learning. Meanwhile, research has progressed in the US, China and Europe<sup>9</sup> on quantum computers. IBM in the USA and Alibaba in China have

already built prototypes for cloud-based quantum computing for experimental purposes.

If quantum computers were actually to leave the lab one day and come into daily practical use, they would be a revolutionary innovation. They would revolutionise communication, sensors and navigation – to name but a few areas. Quantum computing makes primary use of two quantum mechanical phenomena: superposition and entanglement.

Superposition describes a combination of states. While conventional computers require the data to be encoded into binary digits (bits), each of which is always in one of two definite states (1 or 0), quantum computers use quantum bits or qubits that can be in two states at the same time. One application scenario is the utilisation of an enormous computing power to swiftly decrypt data that was safely encrypted by previous standards. This would have far-reaching implications for communication flows and critical infrastructures such as finance. Data stored and non-decryptable to date could be disclosed in one go – a nightmare scenario not least for intelligence services.

Entanglement describes the phenomenon that two or more particles (for example, photons) always assume the same state, even across large distances. In concrete quantum cryptographic applications, this allows the secure exchange of information. The information exchange is secure because the quantum mechanical entanglement makes it impossible to tap the communication link without the interference being easily noticeable – in other words, eavesdropping is ruled out in quantum cryptography by law of nature. As early as in 2016, China launched Micius, the first “quantum satellite”, which was used to demonstrate a quantum cryptographically secured video call between Beijing and Vienna. China, the US and Europe are currently developing fibre-glass-based prototypes for a “quantum Internet”.

A third example of a relevant use of quantum computers involves extremely precise sensors. In particular, Washington is worried that the US stealth supremacy might be abruptly nullified by China’s lead in the use of quantum radar.

Quantum computers have so far been laboratory experiments that have not been of any significant economic benefit, not to mention military use. It is uncertain whether and how their use can be scaled and generalised. Nevertheless, it is worth keeping an eye on the field. Even if limited to a small number of special applications, their parallel operation with conventional computer infrastructures for military purposes might cause power asymmetries. Pioneering in the field of quantum computer based decryption and encryption might, for example, mean global dominance in the information domain.

---

<sup>7</sup> See also Metis Study No. 1 (February 2018), p. 4–5.

<sup>8</sup> Example: „You Won’t Believe What Obama Says In This Video!” <https://youtube.com/watch?v=cQ54GDm1eLo>  
Deep fake videos can still be revealed as fake at second glance. In a few years from now, however, it will be impossible to do so without special tools.

<sup>9</sup> In September 2018, the German Government adopted a “Quantum Technology Research Programme” worth approximately EUR 650 million. In addition to the Federal Ministry of Education and Research, the Economic Affairs, Interior, and Defence Ministries also take part in this project.

**Conclusion: Germany in the digital age's world order**

The transformation of data into power by means of technology has an enabling effect, but determines nothing in terms of great power politics. Regarding the world order of the digital age, we must look into how different models of society interact with technological changes.

Over the last two centuries, the steam engine, telegraph, combustion engine and radio have restricted economic and political centralisation. From an economic angle, the Soviet Union collapsed not least because Moscow was unable to exercise centralised control of the wheat crop distribution or to reasonably determine the local price of bread due to a lack of information. Decentralised forms of organisation such as a market economies and democracies historically benefited from this paucity of information. China is showing that the two must not necessarily go hand in hand. We now face the data deluge of the digital age. An excess amount of information rather than a lack of it is becoming the rule. For the first time, centralised, authoritarian systems might have a historical advantage over those in which the centralised collection, processing and use of data is restricted by standards, laws and institutions – the disparities in resistance against civil-military integration, including concrete examples such as the Maven project, between the USA and China fit this picture.

The attraction of such technology-backed authoritarian systems must not be underestimated. Internationally, the majority of states are not ideal democracies by OECD standards. For societies without traditional, well-established relationships of trust, total surveillance combined with social credit systems of the kind currently being tested in China is an attractive opportunity to establish a functioning community without “troublesome” elements of democratic participation and rule of law. In fact, an astonishingly large number of Chinese people appreciate reputation-based social credit systems because they expect them to promote fairness and the fight against corruption.

In addition to this, there are newly emerging technical possibilities for exerting influence on populaces by

manipulating the information domain and thus political decision-making processes – these are other fields in which liberal democracies are particularly vulnerable. The fact that this model of society in the still young digital age is currently under pressure, both domestically and internationally, is a clear warning sign.

The crucial question concerning the future world order from Germany's point of view thus extends beyond security policy. It is this: Can a liberal democracy be maintained and renewed for the digital age together with a social market economy?

A reason for optimism is the fact that the race of the great powers for the lead in digitisation is basically a competition for the best talents – there will be no innovation without them. Liberal democracies, especially the United States, still have the edge over others. China is aware of this and therefore aggressively courts Chinese talents studying or working abroad and urging them to return. Open, democratic, pluralist and market-economy societies based on the rule of law must therefore (continue to) benefit from the attractiveness of their model of society and the chances for civil rights and liberties, security, education and prosperity. If this model is to remain strong and credible in the digital age, it must undergo further development. Three major fields of action arise for Germany's liberal democratic political and social market economy model:

- Development of regulatory systems, to match the information overload with the principles of a liberal democracy and the rule of law by returning control over data to the individual.<sup>10</sup>
- Provision of advanced training to mitigate structural changes in the labour market caused by automation.
- Integration of ecology into the social market economy as a political constant and promotion of this internationally as a guiding principle for countering the social and economic externalisation effects of the market economy (especially climate change). 

---

<sup>10</sup> An adequate response would be open systems that return security and privacy to users and enable them to fully control state and company access to their data. “Solid”, launched by Tim Berners Lee, the inventor of the World Wide Web, is an example for such a project.

**IMPRINT****Publisher**

Pilot Project Metis  
Bundeswehr University Munich  
go.unibw.de/metis

**Author**

Dr. Frank Sauer  
metis@unibw.de

**Art Director**

Christoph Ph. Nick, M.A.  
c-studios.net

**Photography**

Daniel Chen auf Unsplash

**Original title**

*Großmächte und Digitalisierung –  
welche Folgen für unsere  
Weltordnung?*

**Translation**

Federal Office of Languages

**ISSN-2627-0609**

This work is licensed under the Creative Commons  
Attribution 4.0 International License.

