The digital domain is an arena of opportunity for Russia in which to attempt to achieve its various objectives. However, it is also a source of threat, as it contains the possibility of attacks on Russia’s digital infrastructure, including the ability to send a relatively uninterrupted flow of information to the public. The continued development of artificial intelligence has the potential to upset the system, and Russia, which will trail the leading states within this field, is still in the early phases of formulating a response to this challenge.

RECOMMENDATIONS

■ Remember that the digital domain in Russia is seen not only as an arena of opportunity, but also as a source of threat to the state (or rather to the regime).

■ Be prepared for Russia to think creatively to minimize the gap separating it from the world’s leaders in the development of AI.

■ Be prepared for Russia to work for an international regime restricting the use of AI for military purposes.
‘Whoever leads in Artificial Intelligence will rule the world’. So said Russian President Vladimir Putin to an auditorium full of students in September 2017. And in his February 2019 speech to the Federal Assembly, he announced that by 2025 Russia should lead in this field. Putin’s comments alert us to the prominent and ever greater role played by the digital domain in Russian military thinking.

For example, the digital domain is mentioned in most Russian works on hybrid warfare, where it is often seen as a ‘chaos enabler’ (khaotizatsiya), disrupting digital infrastructure and making possible the swift and global transfer of information designed to influence the political views of a target population. Russian commentators often point to alleged Western interference in the 2010-2011 Arab Spring and the 2014 Maidan protests in Ukraine, as well as to the aftermath of both these events, as indicators of how such operations may be conducted.

As such, the digital domain is mainly viewed as a non-kinetic tool, the effects of which may be felt in both the digital domain itself and the cognitive domain. It is also, however, recognized as a kinetic tool, one that may cause destruction in the physical domain, for example, through an attack on the software used to control nuclear power plants.

The potential system-upsetting impact of Artificial Intelligence (AI) is reflected in the debate over these emerging technologies as the key to unlocking a new offset strategy. It is most clearly articulated in and by the USA and follows the earlier offset strategies of nuclear and stealth technologies. Such strategies are defined here as a technological leap allowing a state to enjoy a decisive advantage over second-tier states, even though this advantage is most likely to be only temporary.

Accelerated by the near-breakthrough of AI, the digital domain may be visualized as a space the outer boundaries of which are being pushed outwards at great speed. In other words, it is a digital Big Bang. Most if not all states within this space are racing to the boundaries in the hope of arriving early and being the first to exploit the new opportunities being offered and of being the first to design early defences against emerging threats. While no single state will be able to arrive successfully at the boundaries ahead of the others and thus be able to relax, some states will travel faster than others. The pace will be led by the USA, China and probably others as well. Russia will trail these leading states and, his February 2019 announcement about Russia as a leader in AI notwithstanding, Putin undoubtedly knows this.

Plan A and Plan B
In addressing his student audience in September 2017, Putin explained that ‘it would not be very desirable if [a possible] monopoly [on AI] were to be concentrated in anyone’s hands specifically’, adding that ‘if we become leaders in this area, we will share this know-how with the entire world’. This altruistic gesture is not, of course, to be believed, if only because of the enormous potential of AI within industry. Putin’s comment should perhaps be interpreted rather as an early step towards establishing an international regime to regulate the use of AI for military purposes. If the Russian authorities are concerned about being left behind as AI technology unfolds, self-imposed restrictions on part of a circle of advanced states may be their Plan A.
Regime theory suggests that, while not impossible, any such plan will be difficult to implement. The central problem is verification, in other words, whether there is a way to ensure that states are observing the regime. Verification would necessitate the inspection of software, which may easily be re-programmed, and it is doubtful whether states will allow international inspectors access to highly advanced and sensitive codes. This points to Russia adopting a Plan B.

Under any such Plan B, Russia can be expected to think creatively to minimize the gap separating it from the leading nations. To illustrate, as AI enters the battle space to a much greater extent than we see today, technological laggards will gradually develop doctrines designed to bring battle to highly complex environments, thereby reducing the advantages of AI-guided operations. When combined with a fast learning environment and a very robust strategic culture, current and future elements from the digital domain promise to allow Russia to compensate for some, but clearly not all, of the totality of its deficiencies across the three domains, that is, physical, digital and cognitive.

**Robust strategic culture**

Russian interference in the 2016 US presidential election offers an example of fast learning and a very robust strategic culture. The hacking of servers, the calculated release of stolen confidential data and the use of both regular information and disinformation to influence voters, including through micro-targeting, shows an approach to the use of some of the digital tools available that is both innovative and audacious. Russia leads in neither the development nor the general application of the technologies used, but it found a way to employ them to achieve certain effects nonetheless.

When confronted with these accusations by a US interviewer, Putin insisted that this could easily be faked. “They can make it so that it will be sent from your home address. Your children sent it”. While the digital evidence collected by the US authorities points to Russia, Putin understands that, since the overwhelming majority of people do not understand the complex technology behind this, scepticism of any alleged evidence may easily be fuelled.

Russia should be expected to exploit this problem of attribution to the fullest extent possible and also to design its operations to fall below NATO’s 2014 Article 5 cyber pledge. These challenges will be felt most heavily, but not exclusively, as Russia designs and
executes non-kinetic operations within the digital and cognitive domains. However, as the digital domain becomes ever more central to the execution of kinetic operations in the physical domain – most notably through AI – it will become increasingly difficult for states to hide behind the problem of attribution. There will be a physical footprint which is less easily erased.

Psy-wars and neuro-wars
As already mentioned, the digital Big Bang will offer new opportunities, but at the cost of emerging threats. Authoritarian in nature, the Russian regime is acutely aware of this. Tellingly, the threats identified are mainly within the cognitive domain. The role of the digital domain in this is to provide access points – conveyor belts – into the cognitive domain, making possible the swift and large-scale transfer of ideas to a (Russian) target population. Russia’s 2016 Doctrine on Information Security refers to such processes as ‘information-psychological’ acts, and elsewhere in the relevant Russian literature we find terms such as ‘behavioural wars’, ‘psy-wars’ and ‘neuro-wars’.

The Doctrine on Information Security covers both the digital and cognitive domains. It makes references to critical digital infrastructure – including power grids, banking systems and even ‘military and special technology and automated systems of control’ – and it notes how Russia’s security is being challenged by the ‘increasing ability on the part of foreign states to influence information infrastructure for military purposes’.

The main emphasis, however, is on the cognitive domain, that is, on the flow of information to members of the Russian public both from within Russia and from abroad. Given Russia’s notoriously wide-ranging Law on Combating Extremist Activity, in this reading ‘information security’ is a broad term. It points to flows of information which would be considered fully legitimate in liberal democratic states, but which are seen or construed as threats to the stability of the Russian state (or rather, the Russian regime). It is frequently observed of authoritarian states that their main worry as far as the digital domain is concerned is information, not digital infrastructure.

Internet sovereignty
In February 2019 the Russian Duma approved a draft law on ‘internet sovereignty’ at its first reading. The purpose of the law, so the Duma website explains, is to ‘achieve the hoped-for work on the Russian part of the Global internet, which should be stable in the event of a disruption of the internet beyond Russia’s borders or targeted large-scale external influence’. This Russian internet is known as RuNet and it is ostensibly designed to increase the digital resilience of the Russian state. According to Russian media, a new internet-monitoring (‘early warning’) centre under Roskomnadzor, the Federal Agency for Communications, Information Technology and Mass Media, is to be established by 1 July 2019, and by 1 January 2020 Russia should be able to unplug itself from the global internet if it deems it necessary.

Russian critics insist that in reality ‘internet sovereignty’ is more about internet control than about digital resilience. In other words, it is more about the cognitive domain than the digital domain. They point, for instance, to the existing digital infrastructure within Russia in support of their argument, insisting that the presence in Russia of eleven instances or mirrors of root servers provides adequate access for users. They also argue that RuNet will be vulnerable to infiltration, for instance, by means of a targeted virus, rendering the whole process futile at best. The inspiration seems to be China, where the authorities are engaged in plans similar to those being implemented by Russia, but the latter has less economic means and less advanced technology. It therefore remains to be seen whether Russia can successfully manage to unplug itself.