Russia can select from a very large toolbox when engaging in influence operations. The different tools are all ultimately used in attempts to influence personal views and/or public opinion. Russia’s many activities have put the West on the defensive. However, the digital tools it uses are Western in origin, and Russia is unlikely to assume the lead in developing new technologies.

There is currently a great deal of focus on Russian influence operations directed at the West. Examples range from the spread of disinformation on Russian state-controlled media platforms and microtargeting on social media by pro-Kremlin opinion-makers, researchers and think tanks to the organization of

RECOMMENDATIONS

- Prepare for an ingenious and robust use of the influence operations toolbox on the part of Russia: it is important to think creatively to counter this use.
- Focus on the most important cases: it is impossible to prepare for all eventualities within what is a vast arena.
- Expect international regimes designed to regulate influence operations launched in the digital domain to be difficult to establish and uphold.
- Recognize that cognitive resilience therefore is critical.
The focus is on how to conduct influence operations designed to change norms and preferences within a target audience.

‘Since there is no difference in russophobic approach between #DK Government and opposition, meddling into DK elections makes no sense’

Tweet by the Russian Embassy in Copenhagen, 24 July 2018

street protests and the deployment of motorcycle gangs. ‘Influence operation’ has become an easy catch-all term denoting a variety of hostile though usually non-military acts. The conceptual confusion is regrettable but also unsurprising. The term ‘influence operation’ is, after all, used rather vaguely by Russian theorists themselves.

Influence operations are selected from a very large toolbox spanning all three domains – the physical, the digital and the cognitive. While operations are conducted in the physical and digital domains with the aim of achieving an immediate effect, the guiding purpose is to achieve an ultimate effect in the cognitive domain. This ultimate effect is in turn linked to objectives at the tactical, operational or strategic levels, potentially making these objectives very different in nature.

To illustrate, in July 2018 the Greek authorities accused Russian diplomats of working actively to influence public opinion away from supporting the compromise between Greece and FYR Macedonia over the latter’s name. The compromise on the name ‘The Republic of North Macedonia’ paves the way for this state to join NATO and the EU, adding more weight to what Moscow sees as two hostile entities. The Russian organization of and support for mass demonstrations in the streets of Athens clearly had the strategic objective of preventing this.

Influence is key

The cognitive domain is central. Influence operations should trigger a learning process in a target audience: they should influence. Classical learning theory identifies two different types of learning. These are ideal types: most learning takes place in the space between them.

First there is simple learning, in which an actor (for instance, an individual, a group or even a state) responds to external stimuli in a way that promises to maximize output. This could be to gain benefits or avoid punishment. In other words, a social or material incentive is created, which informs behavior.

Secondly there is complex learning, in which the actor changes fundamental norms and then responds accordingly. In contrast to simple learning, in this case the actor actually comes to believe that the behavior undertaken is correct and not merely the better option.

Most of what is now discussed in Russia under the heading ‘influence operations’ and its sub-category ‘information war’ relates to complex learning. The focus is on how to conduct – or rather, to defend against – influence operations designed to change norms and preferences within a target audience. Much of the theorizing has been done against the background of Western military interventions since the 1990s and alleged support for so-called colour revolutions. There is an underlying assumption that the West has been both aggressive and successful in its operations.

Non-military operations become a priority

Russian writings on the subject of Western operations provide us with insights into Russia’s current thinking about its own possible use of influence operations. Even relatively recently, high-profile Russian military writers have alerted their readers to the importance of the digital and cognitive domains. The standard reference work is a seminal 2013 article by Valery Gerasimov, Chief of the Russian General Staff, in which he argues that, in contemporary interstate conflicts, the ratio between non-military and military
operations should be 4:1. Later writings by leading Russian theorists point to an increasingly central role for the non-military operations. These are to be found in the slightly larger influence operations toolbox, and they unfold mainly across the digital and cognitive domains.

These two domains may be viewed as the ‘big bangs’ of current political and military thinking. This analogy points to two separate domains that expand even as we race towards their respective boundaries. We need to identify the boundaries – that is, map the domains – in order to determine not only how we may make best possible use of them to further our own interests, but also what protections we need from the harmful operations of others. The challenge – and this is also reflected in Russian writings on the topic – lies in the relatively large uncertainty about the continued expansion of these two domains, the digital and the cognitive.

The digital enabler
This expansion is, of course, most pronounced and seen most clearly in the digital domain. The nature of Russia’s meddling in the 2016 US presidential election and the way the US authorities have handled this suggest that both sides have had to learn fast from a relatively poor knowledge base. The Russians experimented with the transfer of particular political preferences to US voters through whatever was available in the digital domain, while the Americans were left scrambling to determine what exactly was available to an external aggressor and how the digital domain was connected to the cognitive domain.

**THE THREE DOMAINS**

- **COGNITIVE DOMAIN**
- **PHYSICAL DOMAIN**
- **DIGITAL DOMAIN**
The main unknown in the digital domain – and the main driver propelling its expansion – is, of course, artificial intelligence (AI). In 2017 Russian president Vladimir Putin famously declared that ‘whoever leads in AI will rule the world’. This announcement gives us an indication of the thinking and priorities within the Russian state-controlled military industry, which will undoubtedly be driving the development of AI in Russia. AI has the potential to revolutionize social life in ways most of us still cannot imagine. As we have not yet reached the boundaries of this domain, we do not fully know what awaits us there.

From the perspective of influence operations, AI will allow not only much more detailed profiling of each and every one of us, but also much better access to our minds. Alarm bells are ringing because of the development, still in an early stage, of AI-fueled Deep Fake, but automated, much more precise and therefore more invasive microtargeting is waiting just around the corner. ‘Behavioral wars’, ‘psy-wars’ and ‘neuro-wars’ are some of the labels now being applied to this development in the Russian literature.

**DEEP FAKE**

Deep Fake is a new type of digital media manipulation. It allows users to manipulate images and sounds to create more advanced and more convincing disinformation. It leaves few or no traces behind that are observable by the public.

The cognitive domain is expanding, albeit at a much slower rate than the digital domain, as we learn more from behavioral psychology about human decision-making. These insights may easily be applied on the ‘dark side’ as well and used for marketing and political purposes to maximize sales or power respectively. Research into decision-making is, of course, also being carried out in Russia, including by research institutions run by the military, and interested readers may, for instance, still work on ‘reflexive control’ in the literature, that is, on the Soviet-era complex learning concept addressing the problem of making individuals arrive at decisions that have been pre-defined by others.

**Russia’s weaknesses**

Given the vague nature of the concept, it is easy to see Russian influence operations almost everywhere and to overestimate their effect. Both assessments are counterproductive. However, for a number of years Russian theorists have been advocating influence operations as a way for Russia to compensate for its deficiencies in the physical domain especially. And what we have witnessed is a strong focus on alternative and maximally cost-efficient ways of achieving the objectives defined. The use of, for instance, social media has demonstrated ingenuity, and the use of state-controlled media platforms has been robust, as disinformation is served to global audiences with little or no hesitation.

Russia has two weaknesses. First, much of what are now being identified as Russian influence operations conducted in the digital domain use Western technology. Indeed, the Russian authorities have put technology that is already available to unexpected uses. This may offer little consolation, but it should serve as a reminder of the fact that it is often possible to anticipate the dots – and to connect them – by thinking more creatively.

Secondly, there is little to indicate that Russia will ‘lead in AI’. Given its heavy top-down and state-controlled Research & Development profile, Russia should be expected to trail the USA and possibly other states as well. It will, of course, adopt new AI technology – and rapidly – but it is unlikely to be a frontrunner. As other states draw closer to the boundaries of the digital domain, this may be bad news for Russian influence operations.