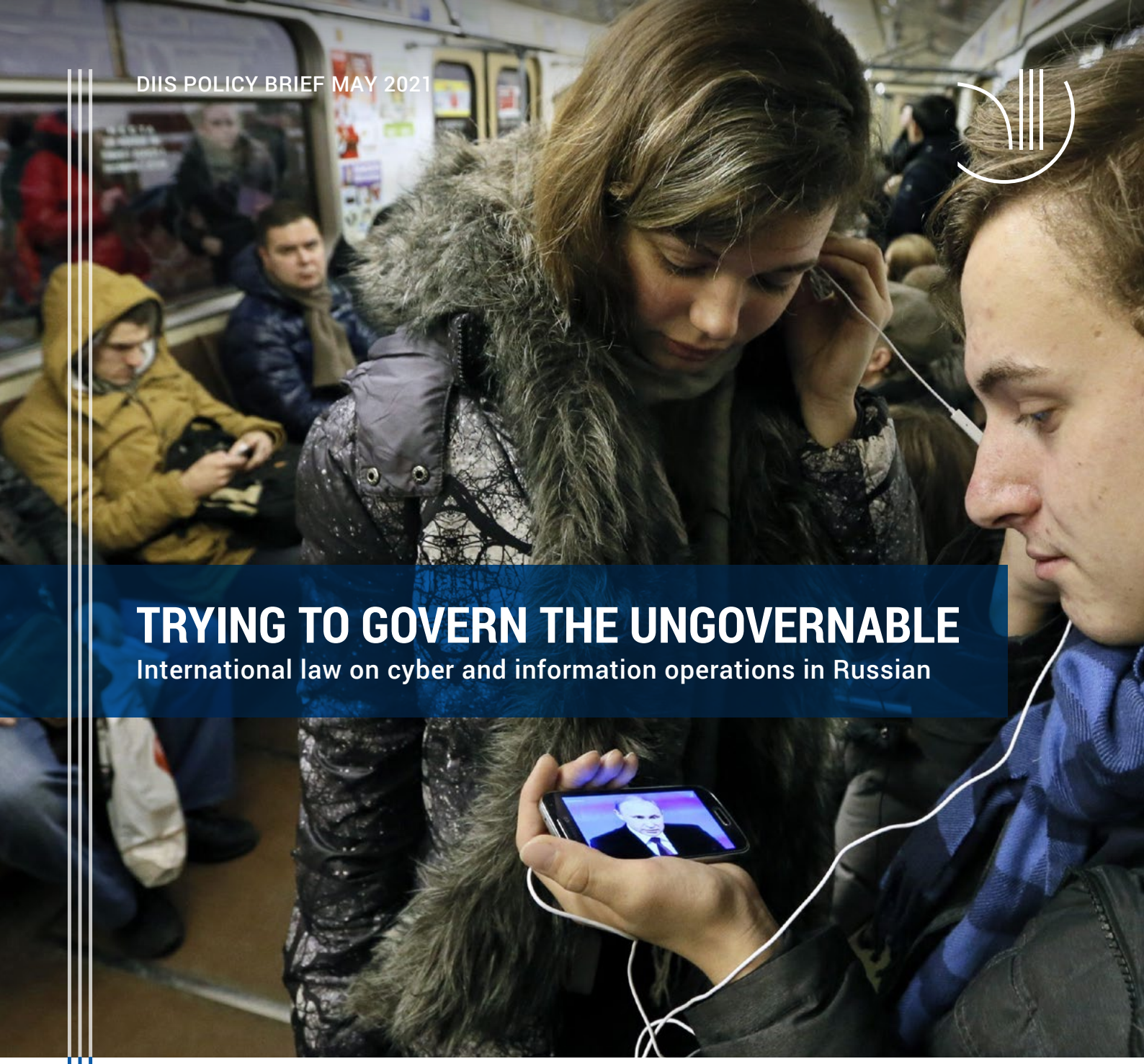


TRYING TO GOVERN THE UNGOVERNABLE

International law on cyber and information operations in Russian

Russia has proposed an international regime governing the use of cyber and information operations. However, 'digital sovereignty' means something very different in Moscow than it does in Washington.

In September 2020, the Russian authorities launched a new initiative to regulate the use of cyber and information operations by states. The Russian President, Vladimir Putin, introduced the debate by suggesting that Russia and the USA lead the way by signing a bilateral agreement restricting their activities in the field of Information and Communication Technologies (ICTs). The two states, so Putin

RECOMMENDATIONS

- Be aware that non-democratic states may want to regulate the use of Information and Communication Technologies (ICTs) to restrict the free flow of information.
- Be aware that non-democratic states are likely to take further action to protect their 'digital sovereignty' through international agreements.
- Given the nature of the cyber domain, it is difficult, but not impossible, to establish international regimes.

suggested, should establish regular dialogue and set up a 'hot line'. Putin also proposed a new agreement on cyber and information operations that should 'exchange guarantees against interference in the internal affairs of the other side, including into electoral processes, inter alia, by means of the ICTs and high-tech methods'.

Shortly afterwards, the Russian Foreign Minister, Sergei Lavrov, added more details. In a statement, he drew a dark picture of the world 'facing a real cyber pandemic', pointing to the risk of cyber attacks against critical infrastructure and the interference by some states in the internal affairs of other states. 'It is high time', so he claimed, that the international community agreed on a regime to regulate the use of ICTs. Russia has proceeded to promote the new initiative at the current 75th session of the UN General Assembly, which has responded with a decision to renew the mandate of the open-ended working group on the security and use of ICTs in 2021-2025.

Russia is a leading cyber power

Russia is generally considered to be a leading cyber power. For instance, the National Cyber Power Index issued by Harvard University ranks Russia fourth in overall capability, behind the USA, China and the United Kingdom. Russia is found to be relatively strong in offensive cyber operations, the surveillance of its own citizens and information control. The first relates to the international arena, while the other two are concerned with the domestic arena, especially regime stability. Remarkably, the Index suggests that Russia is relatively weak when it comes to defending itself against external cyber operations and developing standards of behavior. This ability (or lack thereof) is relevant to the pursuit of an international regime regulating the use of ICTs.

The Russian initiative comes against a background of well-documented use by Russia of both cyber and information operations against other states to achieve certain effects. This represents the offensive dimension measured by the above Index. The most prominent example is arguably Russia's alleged interference in the 2016 US presidential election, which relied on both cyber operations to hack otherwise closed data systems and media platforms to shape the political preferences of voters. Russia's use of these cyber tools demonstrates a relatively robust culture within both the cyber and cognitive domains. It should be added that Russia denies any involvement in these operations.

> The state as a whole should have the right to independently manage its information space, since this is one of the signs of sovereignty.
>
> (Dmitry Medvedev, 12 August 2020)

Seemingly, Putin's initiative to enter into a bilateral agreement with the USA to prevent intervention and interference in the cyber domain runs counter to Russia's interference in the US presidential election. Putin's proposal for such an agreement is not entirely new. Russia has for many years tried to establish universal regulations for the internet. In 2011, it suggested a convention on international information security, which would ban the use of the internet for military purposes and for overthrowing foreign regimes. It was Russia's objective that the convention should reflect the principle of non-intervention in other states' information space. Furthermore, Russia has on many occasions proposed a framework agreement on cyber-security and non-interference with the USA.

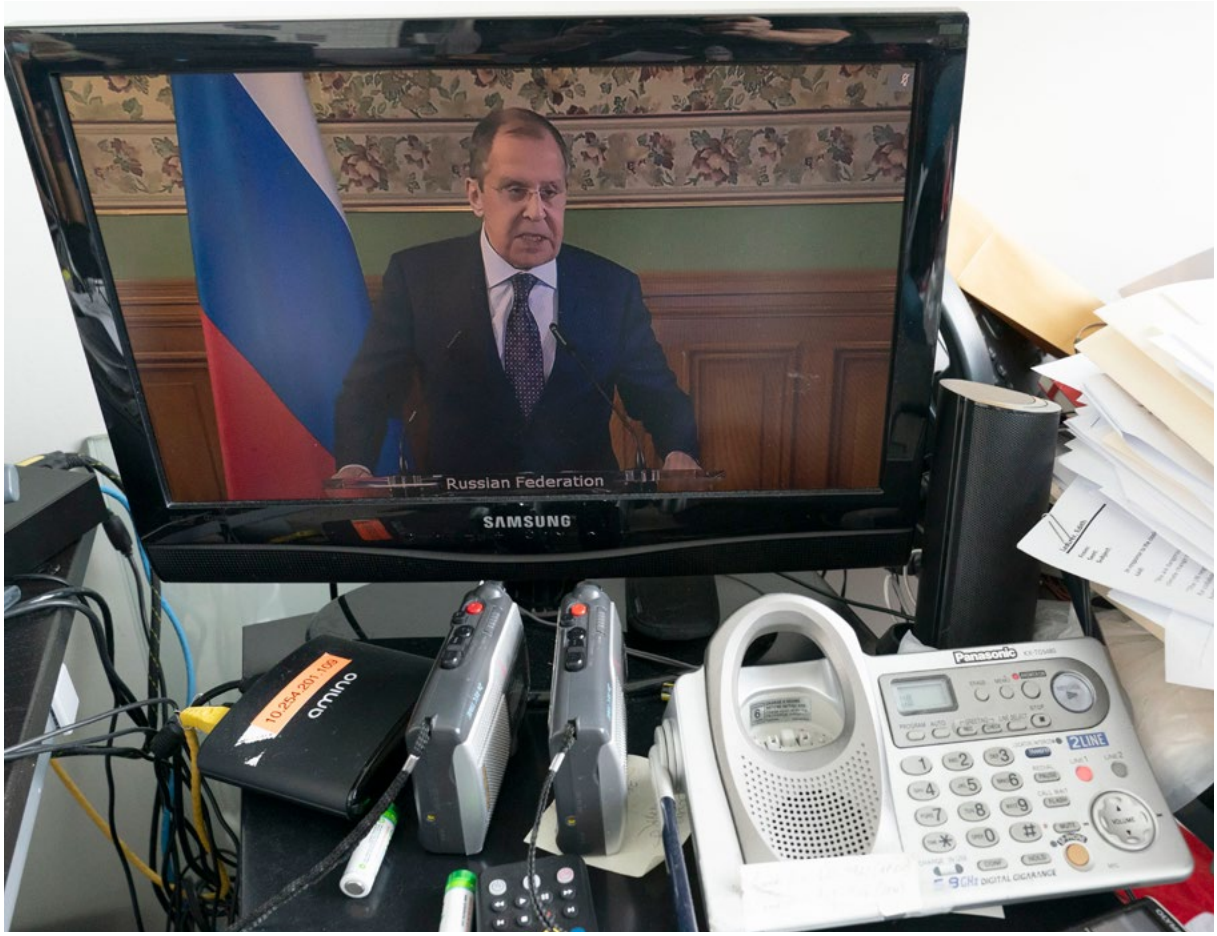
Russia's legal perspective on non-intervention is, however, different from the Western understanding of the same principle. For instance, the free flow of online information in cyberspace is considered a risk to Russia's political stability and to its regime.

In October 2020, a month after the release of Putin's initiative, Lavrov announced that the USA did not want to enter into a non-intervention agreement with Russia, as the 'US[A] itself has long been interfering in the situation in Russia'. It is likely that Russia regards its intervention in the US election as legitimate under international law, as the USA has also been accused of intervening in other state's elections. This position could be explained with reference to the 'clean-hands doctrine' under international law, preventing a state from making claims against another state when it is guilty of the same offence it is complaining about.

'Digital sovereignty': a path to information control

Russia's initiative also comes at a time of rapidly increasing concern within the regime about domestic vulnerabilities in both the cyber and cognitive domains. Relatively weak in defense, the Russian regime has taken significant steps to bolster its control over these two domains. The introduction in 2019 of a sovereign Russian Internet, the so-called RuNet, is a prominent example of this, as it is designed to give the Russian authorities the ability to separate the country's critical digital infrastructure from the global internet. RuNet could also be used to control information flows, limiting or even preventing online interaction between Russian citizens and foreign actors. In January 2021 Dmitry Medvedev, former Russian president and now deputy chairman of the Russian Security Council, announced that Russia 'is ready' to disconnect from the global internet.

Equally far-reaching is the news, released as Putin launched his initiative on ICTs, that Russia is aiming for the development of a national 5G network. A critical Russian commentator predicted that this development would take a long time and be expensive. The decision reflects Russia's lack of trust in existing



Russian Foreign Minister Sergei Lavrov speaks at a virtual high-level meeting of the Security Council on safeguarding international peace and security and global governance in the post-COVID-19 era during the 75th session of the United Nations General Assembly on Sept. 24, 2020.
Photo: Mary Altaffer/AP/Ritzau Scanpix

providers, both Western and Chinese. A considerable amount of uncertainty surrounds this development, in particular over its likely technological outcome. If Russia acquires 5G capacity below that enjoyed by other major actors, it could have serious consequences for its digital defense. National digital autonomy could come at a high price.

Russia has traditionally endorsed the principles of state sovereignty and non-intervention under international law, which prohibit states from intervening in the affairs of other states. Russia's conception of 'digital sovereignty' in cyberspace, however, is fundamentally different from that which prevails in the West. Russia wishes to place more authority in the hands of the state to control cyber activity within its jurisdiction.

Thus, Russia is not a party to the Budapest convention on cybercrime, as some of its main provisions, such as cross-border access to data for criminal investigations, are considered to run counter to the principle of state sovereignty. Instead, Russia has unsuccessfully tried to promote new global agreements on cyber security and cybercrime.

Another example of Russia's view of 'digital sovereignty' is Putin's criticism of the USA's use of cyberspace to collect intelligence. Following the leak of classified information by the former US intelligence employee Edward Snowden, Putin claimed that cyber espionage is 'a direct violation of a state's sovereignty, an infringement of human rights and an invasion of privacy'.

This statement is significant, as it has still not been agreed whether or not the use by states of cyber espionage or other forms of cyber intrusion constitutes infringements of the target state's territorial sovereignty. Seemingly, Russia adopts a view of sovereignty in cyberspace that prohibits all forms of cyber intrusion, including cyber espionage. However, this statement contradicts Russia's own use of cyber espionage, such as the 2020 hack of the SolarWinds software company, alleged by the US authorities to be an operation executed by the Russian Foreign Intelligence Service, the SVR.

In brief, for Russia 'digital sovereignty' is a natural extension of traditional national sovereignty, only this time in cyberspace, where the state can exercise control over the internet. This approach to 'digital sovereignty' is diametrically opposed to the more internationalist approach led by the USA, where the internet is seen as a stateless environment with free access to information and freedom of expression. It is therefore less likely that the USA will enter into any form of agreement with Russia on international cyber security and non-interference if Russia continues to hold a substantially different view from the USA on the meaning and goal of international cyber security. Furthermore, it is likely that distrust between the USA and Russia regarding the other side's use of the cyber domain may stand in the way of an agreement so long as both states accuse each of engaging in cyber espionage and influence operations.

Authors: **Asbjørn Thranov, PhD student (asth@diis.dk) & Flemming Splidsboel Hansen, Senior Researcher (fsha@diis.dk)**

Cover photo: A young couple watch Russian President Vladimir Putin's annual news conference on a mobile device in Moscow's metro, 2014. Photo: Yuri Kochetkov/EPA/Ritzau Scanpix