CSi

The Cambridge Security Initiative

# NO RUSSIAN INTERNET 'KILL-SWITCH' ANYTIME SOON

**NOVEMBER 2019**

**Dr. Victor Madeira**

The Russian Federation's new 'sovereign internet' law came into effect on 01 November. Officials describe it simply as measures to centralise control of and isolate the Russian Internet (RuNet) in unspecified national emergencies, e.g. external cyber-attack, whilst allowing websites and services hosted in Russia to keep working. But the so-called 'kill-switch law' currently faces technical and financial obstacles to full implementation. This means the new legislation, at least in the near term, is more about domestic surveillance and online monitoring.

Proposed changes include giving state communications and media regulator *Roskomnadzor* exclusive crisis-time control over the RuNet, to isolate it from abroad; forcing Internet service providers (ISPs) to install deep packet inspection (DPI) equipment so *Roskomnadzor* can now constantly monitor content and bar any of it without warning; and blocking virtual private networks (VPNs) sold by companies unwilling to help *Roskomnadzor* stop 'undesirable' content.

For now, implementing a complete internet shutdown is virtually impossible. The chance of one depends, for example, on a country's number of ISPs: the higher it is, the less vulnerable the country. One estimate gives Russia 43 ISPs, compared to the U.K.'s 52, putting both in the global top 10. Russian experts have also argued that creating a single bottleneck (i.e. *Roskomnadzor*) would actually make Russia more vulnerable to cyber-attacks. One alternative could be to wall off parts of the national critical infrastructure instead. And suspicions of corrupt bureaucratic turf wars add to the confusion over who will pay for the 'sovereign internet' and how.

All this has potential implications for anyone either operating, or with a client base, in Russia. New DPI equipment greatly improves state monitoring and surveillance capabilities, making confidential communications far more vulnerable (e.g. between lawyer and client, or regarding valuable intellectual property), especially now that VPN companies will be either banned or co-opted by the state. *Roskomnadzor* is also targeting encrypted email providers.

Cutting off the internet would of course have an immediate impact on the financial, energy, and online retail sectors, among others. Economic losses could be significant, but this is something Moscow has in the past shown it is prepared to pay, regardless of impact on citizens. In time, consumers and businesses may bear some of the costs of 'sovereign internet' infrastructure upgrades, in the form of higher prices and poorer service. Firms should also consider their data protection obligations in light of the new law: financial penalties for violations are on the way.

## OUTLOOK

In the near term, the Russian government will focus on rolling out more monitoring equipment, testing its effectiveness and implementing lessons learned. Current technological and financial obstacles to a fully-working 'kill-switch' are such that Moscow will concentrate its newly-acquired capabilities on monitoring internal dissent and preventing civil society from posing any credible, organised challenge. But if, for example, international tensions suddenly increase, Russia may have the political imperative to solve technical problems faster, and accelerate the implementation of something closer to an actual Internet 'kill-switch'.