KCS Group Europe

“My land’s only borders lie around my heart!”

In a video clip a few years old, Russian president Vladimir Putin can be seen handing out prizes to a group of geography students. He asks one the question, where do the borders of Russia end? When the child cannot answer, Putin smiles and says, Russia has no borders. For a President more typically given to visual displays of might rather than the verbal, this might seem a throwaway comment, but, planned or not, there is much truth in what Putin says. Through soft power, there is a concerted attempt to extend power of nation states to the detriment of others, and to move, if not the physical borders, then the goalposts by which the borders (and what they mean) are defined.

This is the age of the rise of the decentralised nation-state: becoming more fragmented than ever in the methodologies and means by which they pursue an agenda, something made all the easier by the increase in technological capabilities and overreliance. Long have states looked to use covert action through technical means to achieve an objective: consider the 2007 shutdown of Estonia’s internet or the virus unleashed upon Saudi Arabia’s Aramco by Israel in 2012. But increasingly the dividing line between a ‘state’, and those they enfranchise to accomplish deeds on their behalf, is becoming blurred.

Microsoft has accused the Russian state-sponsored group Fancy Bears of hacking into the company’s ‘Internet of Things’ devices – this being the same group that are believed to be responsible for cyber-attacks against multiple worldwide government departments. State-affiliated hackers from Russia and North Korea are understood to be targeting key elements of the US 2020 election campaign. China’s very own APT10 group, purported to be a front for the Ministry of Security, is believed to have been behind a concerted effort to attack US utility and energy firms.

Two points of interest from just this very small and recent sample: notably all of these are crucial industries, meaning that the attacks can be debilitating in and of themselves, or *‘testing the waters’* for something deeper to come. But also, in each case (and plenty of others) the actual actors were not explicitly the states, but groups which at best could be allegedly tied/affiliated to, or funded by… but crucially not part of the official state architecture. While it is well known that all major states employ official cyber divisions, to not even use them in matters such as this is a major signal of intent: they know that they have others.

This in turn affects the strategies and options available to the states themselves (perhaps the ultimate bad actors). In the great game of geopolitics every state attempted to force their advantage, and every state knew that every other state did this, and knew about them in turn. But using third-parties as obfuscating and entirely deniable chess pieces is a new frontier because it will rarely be able to be said with absolute certainty that these are state actors: thus the power (both actual and diplomatic) to rein them in is lessened, and the more ability these pieces will have to advance across the board.

And this is where we come to the concept of expansion of borders. If the days of territorial control through expressions of hard power (such as an army) may be dying – although certainly Ukraine and Kashmir would have something to say about that – it is in the extension of power across borders, and an increased ability to act inside them, that the concept of a secure nation-state begins to look shaky. Moreover, if the lines of what constitutes state action are no longer defined, then we do indeed have situations where actors across borders dilute the very concept. And the consequences for the security of our public bodies, corporates and institutions will be dire.