KCS Group Europe

A month of war

The Russian invasion of Ukraine is quite rightly dominating the discourse at the moment, in every sphere. The most common phrase doing the media rounds for the past month has been 'Putin's war'. This is both a confirmation of the degree to which this war is being authored by one man, and a tacit acknowledgement that an increasing number of Russian citizens – and perhaps political and military figures as well – do not support the conflict. Most of the analysis has focused on Putin's ultimate responsibility for every atrocity meted out in Ukraine, and certainly, he has joined the ranks of the modern-day war criminal club. But of equal focus is the second word – '*war*'.

Unarguably, the invasion represents a significant step up in Putin's calculations and willingness to act, and the severity has been matched by the response that was far more muted during the brief incursion into Georgia in 2008, or since the annexation of Crimea in 2014. The impact has been brought home to us, perhaps for the first time. But a more realistic view of the situation would be to say that Russia has effectively been at war with the West for decades, it is just that it has not been a war fought with tanks and bombs, until now. This is seen in the interference in the US presidential election of 2016, it has been seen in the professionalisation of cyber-attacks dating back at least fifteen years, and it is seen in the practice whereby Russian corporates abroad operate as political, and economic, arms of the state. Arguably, the Cold War did not stop when the Berlin Wall fell, and we are now entering a new era of hostilities – one where the battle lines are murkier than ever and increasingly, corporates find themselves at the front.

Russia was unprepared for just how unified the West would be in its condemnation of the invasion, nor how severe and wide-ranging the response. The 'headline act' obviously is the new round of sanctions but there is an effective diplomatic, economic, and cultural boycott as companies and governments alike rush to disassociate themselves from anything Russian. Moscow has essentially made itself a pariah state not just for the duration of the war, but perhaps for generations to come.

Not only is the military conflict likely to continue for far longer than Putin had planned for, with each day bringing fresh horrors and further condemnation against Russia, but the chances of rapprochement diminish too. Neither Russia, nor the companies in her markets, can sweep this under the carpet and pretend that normality has returned.

In the immediate term, clearly business-as-usual in Ukraine is impossible, and in Russia ill-advised, given the prevailing attitudes towards being seen, even tacitly or implicitly, as endorsing Putin's war and propping up the regime. Any in-country business would be advised to stop immediately, although this is not always possible. Any Western business still in Russia will find itself facing reputational questions, to say nothing of operating in a market where the default mode is now to mistrust and punish the West more than ever. So, we shall confine ourselves to the fallout and pushbacks arising as a Russian response to the new environment.

Putin will respond in three ways:

1. Defensive. Facing an exodus of foreign business and investment from Russia, and the tanking of the rouble, the Russian finance ministry moved quickly to claim that any business voluntarily stepping out of the country would be akin to declaring 'bankruptcy', with directors liable for criminal charges. Putin also spoke of simply creating any new laws that might be needed to further limit, or punish, the firms leaving Russia. Any interests remaining in-country, whether you are looking to reduce them or not, will now be targeted. This also makes it very difficult for firms to return after – as is a theme of these entire remarks, Putin views everything now through the prism of 'us versus them' and so one immediate impact on businesses is essentially having to decide their Russian policy for the foreseeable future.

2. Stealthy. Just as Russia has been exploring the public limits of its soft power for a while now – see the 2018 World Cup, or the Sochi Winter Olympics – so too has it been acting behind the scenes to extend its power and influence throughout the political and corporate worlds. The UK alone has come under intense criticism in recent weeks for being a laundromat for the wealth of Russian oligarchs and corrupt elites, to say nothing of the degree to which their financial donations and connections were warmly welcomed by the government over the past decade. These ties also are being shut down, which means Russia needs to get more creative with how it exerts control. We can, for instance, expect Politically Exposed Persons to use proxies, shell firms and the like, to continue to wield power behind the scenes, but the paper trails will become more obscured, and transparency diminished. The risk to companies is that it will be less clear than ever that they may ultimately be doing business with sanctioned or otherwise controversial entities, with damaging and potentially fatal consequences should this be revealed after the fact.

3. Offensive. Russia has never been afraid to be aggressive. In recent years, this has manifested itself in extensive use of cyber techniques to steal from, manipulate and otherwise disrupt foreign companies and governments alike. We have already alluded to the US election interference but would also point to the attack in 2007 that brought down Estonia's government and corporate

infrastructure, or the NotPetya attack that crippled much of Ukraine's political and corporate entities a few years back. It is well known that entire divisions of the army are given over to creating and launching new forms of offensive malware and other cyber-attacks, and that groups of civilian hackers are effectively state sponsored in service to what has been called 'patriotic hacking'.

This is just as valid a form of warfare, in Russia's eyes, as the traditional kind, and may even be more effective in the long term. Rather than the binary nature of armed conflict, cyber allows not only for deniability – although not always plausible – but enhanced capability to disrupt and target those it considers enemies without having to actually show your colours, so to speak. Consider the events of autumn 2021 where the Pentagon, CIA, nuclear research laboratories and Fortune 500 companies were all subject to intrusion and data compromise by Russian hackers. If this isn't warfare, what is? All because Russia is not sending tanks and missiles into America and the UK, does not mean that she is not looking to actively disrupt and damage those nations as much as possible through whatever means it deems necessary. This is particularly true of critical industry and infrastructure such as telecommunications, utilities, and financial institutions.

Indeed, the UK government has put British financial institutions 'on alert' specifically against both Russian ransomware for financial benefit, and data-wiping malware that causes irretrievable losses. These represent the twin rationales of the Putin mindset: we will benefit from you <u>if</u> we can, but we will damage you <u>because</u> we can.

This brings us back to the idea of the 'corporate front' and that American and British firms will bear the brunt of Russia's assault on the West. Speaking from a cyber-perspective, sometimes this will be for an explicit purpose, such as the theft of a specific piece of data or for the financial reward, but it can also be purely as a proof of concept or a warning: that Putin has the capability to take down Western infrastructure networks or cripple businesses. These are ultimate messages to the government, but it is the corporates – who will have fewer and weaker protections compared to those governments – who are the victims.

President Biden's recent remarks bear this out – that Russia is looking to conduct cyber-attacks on the US both as a direct response to the sanctions, and as a warning should the West go further. It is telling that he specifically called upon 'companies' in the general sense to improve their security posture, suggesting that Russia is planning to attack via ransomware, denial-of-service or other malicious malware indiscriminately at the heart of everyday life rather than going for the rarefied governmental targets.

Putin has already commented that opposing nations would face a threat 'like none they had ever seen' – if one assumes for the moment that nukes are out of the question even for him, and that explicit military

action against NATO is not going to happen, cyber-attacks are the most devastating third way possible. NotPetya caused $10bn USD of damage worldwide, and Russian capabilities have only risen since then.

But also, the threat profile for companies is raised through traditional means as well, no matter where they work or what they do. Not only is this building upon standard Russian practice of infiltration and silent control – for instance, one of our cases a few years back involved an FSB agent who had gained virtual control of a key foreign port facility through a proxy company – but that there will be an extra layer of response & revenge added on because of the lost business that Russia will now not get. If you were an oil & gas firm pulling out of Russia to do more work in, say, Dubai instead, it is very likely that Russia is going to try and still keep a finger in the pie through proxies and shells, or to punish you for making what will be seen as a binary choice: Russia or the rest of the world.

It is also important to point out that, from the cyber side at least, the threat profile will not always be Russian – or not appear so. Three examples: the hacktivist collective Anonymous earlier this week leaked sensitive Nestle data as a result of their refusal to pull out of the Russian market and threatened the same for any company that still remains in Moscow. There have been recent intimations that a Chinese cyber-group has hacked the Ukrainian government so as to offer Russia further support and deniability, with the possibility that this could extend to corporates. And scams pertaining to fake fundraising and projects for Ukrainian refugees have already started to take hold online. All of these represent enhanced threat vectors that have come about as a direct result of the Russian war yet are not explicitly Russian in origin. They illustrate that the breadth, depth, and severity of advanced, persistent cyber-threats has only increased on all fronts as a result of what is happening.

As we go forwards, this will be – to quote another common phrase – the ‘new normal’. Relationships with Russia cannot and arguably, should not be ‘reset’, even if a peace deal is hammered out and the violence stops. Putin cannot hope to return to the international diplomatic and economic table without accepting responsibility and the consequences that come with it, and the chance of this is nil. Indeed, Putin’s personal position is arguably the worst it has been since he came to power. He failed to bring about the lightning-fast military victory that was expected, he was proven wrong in the assumption that the native Ukrainians would welcome the Russian forces as liberators rather than conquerors, and he has arguably driven the West away from Moscow’s oil & gas, on which so much of Russia’s soft power, and economy, has depended. Backing down is not in his nature.

So, we can expect a much more heightened threat profile from Russian actors both covert, and overt, and through traditional and cyber-means, to become standardised as Putin – faced with increasing isolation -

responds by playing to Russia's remaining strengths: her ability to hack, interfere with and otherwise damage Western businesses.

To return to the original contention that this is a state of war. This is not hyperbole. For Putin, it is a war of ideology, his contention that Ukraine should not exist as an independent nation absolutely central to the invasion, and the cornerstone of his belief that Russia, must once again, reach the heights of power and influence enjoyed by the Soviet Union. It is for him a fundamental question of reversing a perceived decline, and any means, and victims, are 'fair game' in achieving this. On the other hand, for the West, it is a war of democracy and accountability – that if Putin takes control of Ukraine today, the remaining former Soviet states that have set their path away from Moscow over the past thirty years may be next, and that no longer can Russia be allowed to hack sovereign nations, damage the lives of ordinary citizens, and conduct global financial laundering with impunity. This may be a struggle for systemic survival more than either side would like to admit.

One final note. The past two months have shown significant 'intelligence successes' from Western agencies, not only in predicting the invasion but in how it has developed. On the one hand, this is a sign to take Biden's recent warning about the increased risk of cyber-attack extremely seriously, but on the other, it is a reminder that intelligence works… that it can tell you what you need to know. So use it! If you need specialist due diligence to advise you if your new partners may be puppets for Russian Politically Exposed Persons or sanctioned, take it. If you need enhanced cyber-monitoring and defence to give early warning of actual and potential threats, embrace it. The risks posed to corporates' financial standing and ability to operate as a direct consequence of the invasion of Ukraine mean that the general threat picture is significantly higher than it was at the beginning of the year. We recommend every possible measure in raising your defence to match it.