BEYOND blue
NEWSLETTER
March 2022

CYBER RESILIENCE IS NOW MORE IMPORTANT THAN EVER

Russia's invasion of Ukraine created a moment of acute risk and uncertainty, one whose impact can be felt far beyond the battlefield or the streets of Kyiv. The world of the 21st century is an overwhelmingly digital one and Russia has proven itself adept at exploiting this fact in service of its own geopolitical and security objectives. For many year Ukraine has been the target of sophisticated and destructive cyber attacks. From the disruption of the electrical grid in Ivano-Frankivsk in December 2015 and then again North of Kyiv in December 2016, to the 2017 NotPetya malware attack, and the widespread deployment of VPNFilter router malware from 2018 onwards.

Before the invasion had even begun, Ukraine had endured a torrent of offensive cyber-attacks. There were numerous DDoS and website defacements against Ukrainian national banks, government websites, and media outlets, attributed to threat groups allegedly linked to Russia's Main Intelligence Directorate (GRU) (e.g., Sandworm Team and APT28). Reports of the use of pseudo-ransomware data-wiping malware WhisperGate and HermeticaWiper were also widespread. Attacks have since escalated, with patriotic political hacktivism on both sides. Anonymous has been targeting Russian government websites and media channels, while the Conti ransomware group has threatened to target Western infrastructure.

This is not merely a problem for Ukraine. As demonstrated by NotPetya, aggressive cyber operations designed with a limited target in mind can be hard to contain. That attack cost millions of dollars to companies across the private sector who were likely not the original intended targets. Most notably, it cost Maersk, the world's largest shipping company, $300 million and Merck, a pharmaceutical company, an eye-watering $1,175 billion after it was forced to cease production of various vaccines. Moreover, it is sobering to consider that the NotPetya attack was a peace time aggression.

Sadly the line between state and criminal actors is not always clear. Russian cyber criminals motivated primarily by financial incentives, can operate with a surprising degree of impunity, and as Conti's recent statement suggests in support of the Russian state.

There is also a further risk of impact for organisations based out of countries which have condemned and sanctioned Russia's actions, particularly countries who are members of NATO. Organisations in the US, UK, and EU member states all look particularly vulnerable. For this reason, the UK National Cyber Security Centre (NCSC), US Cybersecurity and Infrastructure Agency (CISA), and European Central Bank have all warned that organisations based in these regions should improve their online defences.

These calls are welcome and timely. Organisations across the public and private sectors should now be in a state of heightened cyber readiness. More precisely, their focus should be on ensuring they are cyber ***resilient***. Adopting an exclusively risk-based approach can place too great an emphasis on estimating likelihood of events when trying to navigate a threat landscape as volatile and unpredictable as the one we now confront. This can be a bitter pill to swallow. Many would still like to believe that organisational cyber security can be treated as an isolated corporate function, one which can be mastered through careful management of risk and the introduction of proportionate controls. But as the current situation makes abundantly clear, organisational cyber security is increasingly embedded within a broader geopolitical framework over which firms have no control.

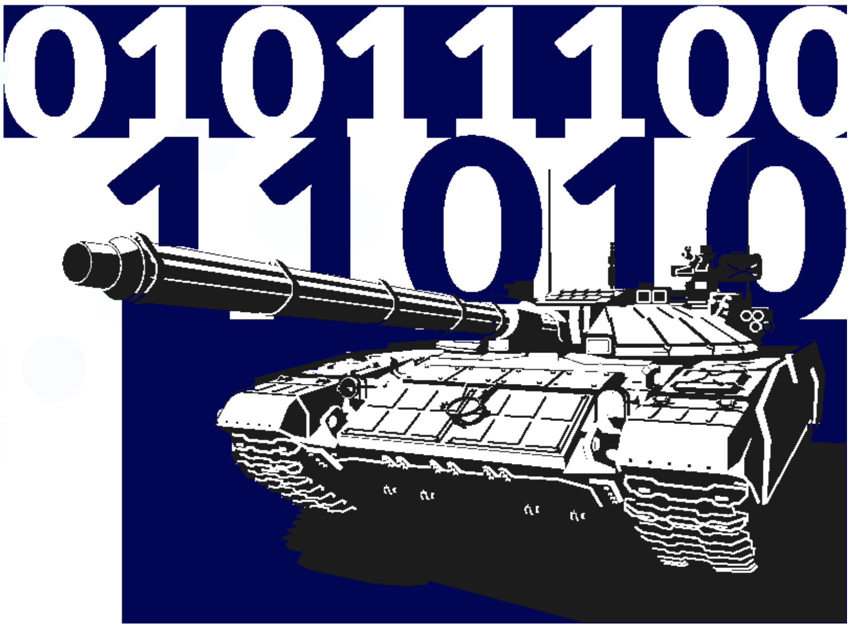
Take time out now to consider how the tragic events in the Ukraine might impact your organisation as geopolitics shifts, perhaps permanently. Cyber security should be part of that consideration, as it is now clear that cyber space has become an increasingly contested space for nations.

Exercising is a vital tool for combatting this uncertainty. Organisations may not be able to predict how they will be hit or by whom, but they can hone their responses and develop a sophisticated understanding of how resilient they are. It is especially imperative that organisations exercise against scenarios that take into consideration their often complex dependencies on third parties and supply chains.

In this forbidding new era, organisational cyber resilience will be more important than ever.

This month's newsletter is dominated by the fallout from Russia's invasion of Ukraine. In our main feature, we consider what this means for organisational cyber security and the importance of maintaining a resilience-based mindset in such a volatile climate. We also consider the government's recent proposals to changes to the Network Information and Security (NIS) Regulations aimed at shoring up the UK's cyber resilience in the face of threats to critical national infrastructure. In addition, we continue our countdown to the deadline for compliance with the PRA/FCA Operational Resilience policy by reflecting on forward planning and development of remediation programmes and we celebrate the reaching of a major milestone by one of the most revolutionary and significant research programmes in contemporary cyber security engineering.

David Ferbrache, OBE
Managing Director



IS THE UK DOING ENOUGH TO ENSURE ITS NATIONAL CYBER RESILIENCE?

In January, the UK government made clear its intentions to strengthen its legislative measures aimed at shoring up the UK's cyber resilience. This marks the first promise of major legislative action in the cyber security space since the introduction of the NIS regulations in 2018 as EU retained law. The proposals come in the form of an industry consultation and focus on two areas of improvement to NIS:

- broadening of the scope of NIS with an eye to minimising the risk to supply chains,
- future-proofing NIS to ensure they are responsive to changes in both the threat landscape and digital technological shifts.

These proposals arrive just over a year after the EU proposed sweeping changes to their Network Information and Security Directive of 2016 with which the UK NIS regulations were originally designed to be in alignment. The EU's NIS2 sought to rectify various weaknesses found in the original directive. One such major concern was the limited scope of NIS, with the Commission citing 'increased digitisation' and 'a higher degree of interconnectedness' as grounds for expansion. Another concern was the inherent ambiguity surrounding which providers of digital services should fall under the NIS remit.

The UK proposals manifest similar concerns about the UK NIS. Perhaps most notably, they seek to rectify the exclusion from regulation of so-called "managed service providers" (MSPs) (i.e., third party providers of digital services such as security monitoring, managed network services, or outsourced business processes). Concerns about MSPs relate to supply chain security. Many MSPs represent a systemic risk given that they are often highly concentrated with a small number of vendors and are also widely used.

Notably, the Government's proposals outline conditions for counting as an MSP which ensure that a very large number of digital service providers (DSPs) will meet them. This generates questions about whether all or only some MSPs should be subject to the same regulatory standards as operators of essential services. The response within the consultation paper is to introduce a distinction between DSPs. On this approach, tier 1 DSPs are those 'essential to the operational continuity and resilience of UK organisations' whilst tier 2 DSPs constitute the remainder. The idea is that tier 1 DSPs and MSPs are regulated in much the same way as operators of essential services, whilst tier 2 service providers are subject to lighter-touch regulation.

On the matter of what criteria of materiality should be used to distinguish tier 1 from tier 2 DSPs, the proposals remain neutral. 8 possible types of criteria are mooted, 4 quantifiable and 4 qualitative. The hope is that the consultation will feed back into these decisions. One issue this raises is whether the ICO's determinations regarding which MSPs fall under the more stringent NIS regulations might have commercial implications. MSPs selected for tighter regulation might be perceived as more secure than those which are not. This could then make them more appealing to potential clients than their less regulated competitors. It seems that the ICO's growing regulatory role will bring additional complexity.

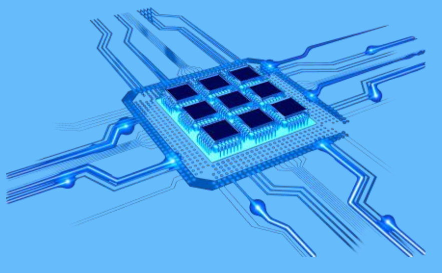
Further to the expansion of NIS to include MSPs and these related additions, the proposals also include the welcome introduction of a host of delegated powers which will enable Government to keep the NIS up-to-date and responsive to fast moving geopolitical and technological changes.

OPERATIONAL RESILIENCE COUNTDOWN

A month from now the first phase of the Operational Resilience policy will have concluded. The focus is then likely to shift to one of the key themes of the next stage, namely, **third parties**, in particular those which are deemed sector critical. The topic of **sector-wide mapping** has been discussed for many years between regulators and financial institutions. The promise is that it would **help identify concentration risk across the sector**. Successful mapping of this kind would assist in isolating technology providers systemically embedded across the sector, critical third parties and, more recently, Cloud Service Providers whose disruption would have significant sector-wide impact. Unfortunately, such initiatives have never gained much traction. The Operational Resilience Policy provides firms with an opportunity to better understand this sector-specific concentration risk via collaborative scenario testing with third parties (a requirement of the Policy) led by industry forums. Competition concerns will restrict the level of detail of such mapping. However, developing a shared methodology and jointly approaching critical third parties has multiple benefits. Most notably, it promises reduced overheads associated with scenario testing on both firms and third parties, a shared view across firms as to the resilience of third parties and, an opportunity to map the dependencies of firms on these third parties. This can provide firms with evidence to the regulators to help encourage bringing the most systemic third parties into the regulatory ringfence.

31
DAYS TO GO

SECURITY SPOTLIGHT



Last month, the UK Research Institute's (UKRI) Digital Security by Design programme reached an important milestone. The programme, which was established to foster advanced academic and industry research into the creation of new, more secure hardware and software, saw one of its major initiatives bear fruit. A consortium of UKRI-funded researchers led by the semiconductor and software design company Arm have made their prototype **Morello demonstrator boards** available to software designers and security specialists for testing. The significance of the Morello boards requires some unpacking. They are the result of a five-year project to develop a working implementation of the University of Cambridge's proposed **CHERI architecture**. CHERI was designed with an eye to dramatically improving system security through a fundamental revision of the design choices in hardware and software. Most notably, it enables software engineers to effectively eliminate **memory safety bugs** (i.e., oversights in a program or language which permit the execution of malicious code via the misuse of variables storing memory addresses). The sheer number and potential severity of bugs of this kind (e.g., buffer overflows) in memory-unsafe languages such as C and C++ give some indication of the significance of this development.

The Morello boards are not intended to serve as the prototype of a commercial product suitable for industrial deployment. Rather, they are a research tool, one that will enable the Arm consortium behind their development to put the CHERI architecture through its paces. Some part of this will be proving that CHERI has certain important properties. Another will be a more granular industrial evaluation of applications of the CHERI architecture in various settings. However, we should not for this reason underplay the significance of what the Arm consortium has achieved. If fruitful, the Morello boards could ultimately pave the way for the development of mass-market CHERI-enabled devices which have the potential to transform the way that computers are designed. It would mark one of the most significant shifts in hardware and software design since the 1970s, and one explicitly designed with security in mind. Watch this space...