Picture credit: US Dept. Defense

TIME FOR CHANGE

Marc Lee *explains why the war in Ukraine should serve as an early warning for the West to reconsider the threat from China and Russia*

Brexit, the pandemic and the war in Ukraine have fundamentally changed the world and how purchasing decisions will be made. What are the issues and why is the private sector now on the frontline? What action can and should the private sector be taking? What action might be forced on it? Cityforum (specialist in policy analysis and public debate) has recently held events to discuss the issues with the leading figures in defence, both in the UK and the US. The insight learned from these, and my own experience, are summarised below. It does not make for comfortable reading.

The seriousness of the current international situation was summarised in alarming fashion by Air Marshal Edward Stringer, former Director General Joint Force Development & Defence Academy & Associate at Cityforum, in April when he said that the current threat from Russia was the worst for 50 years: "The British Government, for the first time that I can remember, since 1962 has had to seriously consider its policy decisions in the light of a possible nuclear exchange." It is not, however, 'just' the actions of Russia that is alarming Western allies. At an event earlier in the year, which was led by Hon. Chris Inglis, National Cyber Director at The White House, speaker after speaker urged the West to be much more cautious in dealings with China.

This is not the first time that the council has confronted a deep division in its ranks

The problem is that too many companies are establishing relationships with China without understanding the huge risks, particularly if you work in the tech sector. President Xi Jinping, who came to power in China in 2013, has a very different attitude to the West than his predecessors. The Chinese strategy is to 'divide and conquer'. George Barnes (Deputy Director – National Security Agency (NSA) – advised that the Chinese are watching how the west handles Ukraine. The ultimate outcome for Russia will inform the Chinese whether the west is strong or weak. If they perceive us as weak, this could galvanise the Chinese into taking action on Taiwan.

CYBER WARFARE

At the same time as the international community is trying to manage these threats, we have woken up to the potential of a new weapon that nearly every civilian has access to. The first World War saw the first use of planes in warfare, the second World War ended with the dawn of the nuclear age. The Ukrainian war will go down in history as the first war fought as much in cyber space as it has been on the battlefield. The teenager operating on a laptop in their bedroom in Hull has been given the power to make a difference in the outcome of the war, particularly if that teenager has the skills of the hacking group Anonymous.

The media has reported wonderfully innovative ways that social media has been used to track Russian soldiers, counter Russian propaganda (through the use of review features on leisure booking sites) and even give money directly to civilians in Ukraine. Anonymous have become heroes by weaponising their hacking to the benefits of the Ukrainian war effort. The public, across the world, but particularly in Europe and the US, has discovered a power that they've not understood and exploited before, and you can see their delight in using it to help bring down the enemy. As civilians we are no longer sat at home unable to contribute.

Of course, our enemies are also exploiting the cyber world. Every time we open our laptops or answer our phones, we now have to defend ourselves against them (as much as we are against fraudsters). Most disturbing of all is that it is very clear to senior people in defence (in the UK and US) that Russian AI is being used to identify, amplify and exploit grievances online, in order to undermine peace. In effect Russia is weaponising extremist ideologies and conspiracies. It is why we're seeing so many bizarre theories gaining traction, despite the fact that they're so convincingly disproven. The militant minority are often not representing the groups they claim to be speaking out for, but have been stirred into action by hostile nations as a highly effective way of breaking down Western democracy.

The only way to protect our values is for the IT community to understand and accept their responsibility in stopping this. Sir Mark Rowley, Former Assistant Commissioner for Specialist Operations Metropolitan Police Service, compared the current legislative challenge of addressing the AI threat, with that of tobacco companies when they posed a threat to health in the Fifties and Sixties, without accepting that responsibility, and to financial services companies, who initially took time to accept their role in preventing money laundering. Tech companies must now take responsibility for their role in spreading disinformation and hatred that helps hostile nations. Sir Mark explained to Cityforum: "This is about the legal aspect of regulating companies and how they act online and what they permit, and I would make a comparison with anti-money laundering."

> **THE KEY CHANGE FOR THE PRIVATE SECTOR IS TO BE FAR MORE CHOOSY WHO WE DO BUSINESS WITH**

Miriam Howe, Senior Security Consultant – BAE Systems – explained; "It's no longer about blaming the users for bad practices, it's about recognising that the humans and systems are mutually dependent and you might target the user to get to the system or you might target the system to get to the user."

China has been playing the long game for some years. Stephen Kinnock MP, Shadow Minister for Defence was outspoken (at the Cityforum event in January) about the lack of caution in the handling of relations with China in the Cameron/Osborne period of government at our event in January. However, other speakers highlighted that the same had happened during the Labour administration.

The weak link in security is often in lack of transparency in the supply chain in privately owned companies and an over reliance on China for investment. The Chinese already own 10 percent of Heathrow and 9 percent of Thames Water and they are deliberately putting money into cash-poor universities. This could lead to unwelcome influence, including screening out critics of China from employment and claims on sensitive intellectual property.

The West needs to be far more careful safeguarding ourselves, while remaining open to exchange and trade. Dr Killworth, Deputy Chief Scientific Adviser for National Security at OCSA, explained how the culture of the designers of technology would influence all our lives and why it was important to maintain our lead in technology. "It matters if a technology is designed in Shanghai, the US or Manchester. Smart city technology, designed under an autocratic state, for example, will rarely protect individual privacy rights by default."

A more mundane, but just as critical issue, is the resilience of the supply chain to manage the threats we're facing. Many sectors have been impacted by the disruptions caused by Brexit, the pandemic and now the war. Technology has been no different. It has taught us to realise that the 'unthinkable' can happen and that we need to plan for it. If you rely on supplies from nations that don't share our values, there is clearly a much higher chance that at some point your supply will be disrupted.

Lord Toby Harris, Chair National Preparedness Commission, explained in April: "One thing that we should learn from the last two years, is that we cannot go on burying our heads in the sand, we need to be better prepared for the unexpected. As a recovering politician, I know how difficult it is for our elected leaders to devote resources to projects that do not come to fruition before the next election, let alone the one after it, or build resilience

THE OUTCOME FOR RUSSIA WILL INFORM THE CHINESE WHETHER THE WEST IS STRONG OR WEAK

that is probably invisible and may never be needed for an eventuality that may not happen.

"The reality is that our cities and communities and our organisations have to have preparedness and resilience designed in, it has to be part of society's fabric. Adopting a preparedness philosophy means parking our 'just in time' approach in favour of 'just in case' and that means being ready to build in redundancy and to avoid interdependence."

In the private sector it is not elections that act as a barrier to an appropriate level of focus on these longer-term issues, but the need to make a profit for shareholders and to survive. However, the recent crises should help re-focus director's minds and appreciate that there is a real risk of sleepwalking into disaster. We can see that in the energy and the car industries, it is already too late to avert the crises they find themselves in. We have to learn and adapt to the new, far less safe and comfy world that we now live in.

The key change for the private sector is to be far more choosy who we do business with, who we rely on and who we let into our supply chain. On the political stage it is clear that we will see a new world where the West will realise the importance of collaboration to manage the threat. However, just as no one country can protect itself, the same is true for companies. We are all part of an ecosystem that has to work better together to keep out hostile elements. We can't continue to simply hope and pray that the worst won't happen, because we can now see it does. International security should be embedded in every decision, whether in the public or private sectors.

Chris Inglis, National Cyber Director at The White House, warned against seeding the initiative on technology to those hostile to our values: "The threats from cyberspace, including from malign actors associated with China are really urgent and, in some cases, severe. As our friends in the UK have shown with the National Cyber Security Centre and their recently released cyber strategy, this will take unprecedented private, public collaboration."

I have no wish to be alarmist, but change must happen at every level before we can return to the safe world we took for granted for so many years ●

Marc Lee is the Founder and Chairman of Cityforum. He spent time at the United Nations and is the author of a book on UN peacekeeping. He also spent time as a Defence Lecturer at Southampton University and is a former Managing Director of FT Business Enterprises.

International security should be embedded in every decision, whether in the public or private sectors

Picture credit: US Dept. Defense