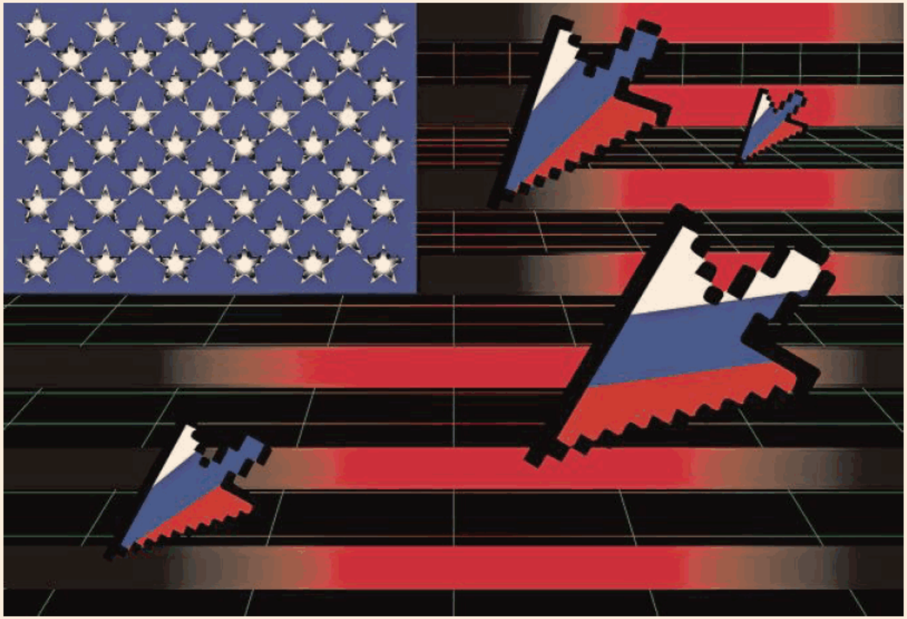
Business finally collaborates on cyber security



Efi Chalikopoulou

FINANCE

Gillian Tett

A decade ago, the Obama White House tried to force American companies to collaborate on cyber defence. It did not go well: the US Chamber of Commerce and other big business groups blocked a cyber security bill, complaining it smacked of excessive government intrusion.

"People said [it] was un-American," a former Washington official says. The mandatory sharing of information about cyber hacks, or devising joint defence strategies, was considered antithetical to free-market capitalist ideals.

How times change. On Wednesday, the White House issued an executive order that requires US companies running critical infrastructure to report cyber hacks. Last month, it summoned senior American executives to launch a collaborative cyber defence project with the ugly name "Shields Up".

Detail is sparse, but it is clear that US business is now collaborating. Investors should watch closely for at least two reasons. The first is that the war in Ukraine means there is a rising risk that Russia will launch a cyber attack on western companies, which could cause enormous damage. In fact, even an assault directed solely against Ukraine could hurt. When Russian hackers attacked Ukrainian infrastructure five years ago by releasing a malware "worm" called NotPetya, it caused $10bn damages to computer systems worldwide with painful consequences for companies such as Maersk, FedEx and Merck.

The second reason to watch these events, however, is a more subtle one: fears of cyber war could contribute to a longer-term shift in the relationship between business and government. Already, once-taboo concepts such as industrial strategy are back in vogue.

Thus far, this shift has not been very visible. Russia does not seem to have launched any large-scale cyber attacks on western infrastructure this year, limiting its onslaught to Ukraine. This has surprised many cyber experts and they are divided over the reasons.

Some think that Russian president Vladimir Putin has deliberately focused on his ground invasion first. "Cyber is not a great tool for warfare," points out Dmitri Alperovitch, head of the Silverado policy incubator and co-founder of CrowdStrike, a cyber security firm. "It's a great tool for grey zone coercion but once you are in a conflict and bombs are flying, then kinetic weapons take over in their effectiveness."

Alperovitch also suspects hackers did not have enough time to craft sophisticated cyber strategies before the invasion, because Putin kept his plans so closely guarded. But Brett Goldstein, a former US government cyber adviser, thinks the more likely explanation is that Putin fears an attack on western infrastructure would trigger Nato's Article 5 clause — and spark retaliation.

Either way, few observers expect this restraint to last. "As the conflict reaches a stalemate . . . Russia's cyber forces may shift focus from attacking targets in Ukraine to instead using cyber weapons to inflict severe damage on western organisations," Swedish consultancy Truesec warns. It predicts "a supply chain attack", similar to NotPetya, where hackers gain access to "the IT system of a large software company and use legitimate channels to push a seemingly legitimate software update to all clients that includes a malicious code".

Alperovitch agrees: "As soon as the Russians think their fortunes are turning they are likely to launch retaliatory attacks . . . [probably] against energy infrastructure in Europe and financial sector in the US."

It is unclear whether western groups can fend off an attack, but a rush to prepare is under way

It is unclear whether western companies will be able to fend off such an attack effectively, but a rush to prepare is under way. "We are constantly sharing information now, in a way we never used to," says the chief technology officer of one large global bank.

Hence the intriguing question of where this attitude shift will lead. After all, the problem is not simply about Russia any more. Threats are emanating from China and other states, creating a challenge Goldstein describes as "cyber MAD". As he notes, "In the 1950s and '60s we applied the concept of mutually assured destruction to nuclear conflict and it worked well as a deterrent framework. [But] how do we land in a deterrent framework for cyber? What does cyber MAD look like?"

The corporate world now sits at the centre of this debate, in sharp contrast to the way things were in the 20th century. That raises a string of thorny questions such as these: should companies ever have the right to keep cyber hacks private? Can they collaborate with each other, without breaching antitrust rules? Can they set their own software strategies and choose suppliers — or should they conform to a government template?

"Increasing the homogeneity of systems and software will increase security," Goldstein notes. "But will that stifle innovation?"

There are no easy answers to these questions. It is far from clear that the US government has the stomach, or the ability, to conduct this debate — let alone implement a unified strategy. But the important point is this: even before the invasion of Ukraine, the relationship between business and government was subtly changing thanks to the pandemic, supply-chain disruptions and climate change. A full-scale cyber attack, if it occurs, will accelerate that shift. There are not many atheists in foxholes, nor blind adherents to the credo of free-market fundamentalism.

gillian.tett@ft.com