A war like no other?

On the eve of the UN-sanctioned invasion of Iraq by a coalition of 35 nations in 1990, the following spoof weather forecast did the rounds: 2 000 degrees and dusty with big cloud expected later. Thirty years have now passed and, following former President George W. Bush's ill-advised 'mission accomplished' follow-up operation in 2003 and current leader Donald Trump's deadly strike in the region, nobody is laughing. **Legalbrief** reports that many are predicting a global war that will see cyber-attacks taking the conflict into unchartered territory. In the early hours of Sunday, shortly after general Qassim Soleimani was killed in an airstrike, Washington issued a security alert, warning that Iran could strike so-called critical national infrastructure such as electricity grids with cyberattacks to potentially devastating effect. Shortly afterwards, **the Federal Depository Library Programme website was defaced by hackers** claiming to be working for the Iranian Government.

While there is no proof linking the hackers to Iran, **Forbes** *reports that if a cyberattack was to hit the US or its allies, it would be accompanied by physical warfare* – the latter of which experts say will probably come first. Discovered in 2010, one of the most sophisticated state enabled cyber-assaults in recent history was the Stuxnet attack on Iran's uranium enriching centrifuging capabilities. **'Stuxnet was blamed on the Americans and some commentators suggested Israeli involvement, which both countries deny,'** said Philip Ingram, a former colonel in British military intelligence. And it had a big impact: it put the Iranian uranium enrichment programme back several years.

From late 2011 to mid-2013, Iranian hackers targeted major banks like JPMorgan Chase, Bank of America and Wells Fargo with large 'denial of service' attacks, making it difficult for customers to log into their accounts and access their money. The banks were overwhelmed by huge amounts of traffic that caused their websites to crash. Seven Iranians were indicted in 2016 by a New York grand jury for the hacking. The seven were employed by two Iranian companies that worked for the Iranian Government. In 2013, Iran hackers infiltrated the control system of a New York dam, raising concerns that American infrastructure could be quietly targeted. **In 2018, nine Iranians were charged with hacking hundreds of universities and companies to steal their data and intellectual property.**

Iran, alongside Russia, China and North Korea has been identified as one of the major state sponsors of cyber-attacks targeting the West but, so far, the damage caused by its hacking has been limited. The US was forced to issue an emergency cyber security directive last January in response to an ongoing attack during the government shutdown. **Sky News** reports that Iran was also blamed for a wave of cyber-attacks which targeted key parts of the UK's national infrastructure, including the Post Office. The vast majority of these hacks appeared to be about espionage as hackers were attempting to monitor and track specific individuals for operations believed to serve Iran's national security strategic objectives. **CNN** reports that the head of the US cyber security and infrastructure agency stressed that **companies need to 'brush up' on defending against Iranian regime hackers.** Acting Homeland Security Secretary Chad Wolf has issued a new National Terrorism Advisory System bulletin in the wake of the drone strike. 'Iran maintains a robust cyber programme and can execute cyber-attacks against the US,' reads the bulletin, which expires 18 January.

In another development, the US Army has banned the use of the hugely popular short video app TikTok by its soldiers, labelling it a security threat. The army has joined the navy in barring the use of the app on government-owned phones, following bipartisan calls from lawmakers for regulators and the intelligence community to determine whether the Chinese-owned app presents a security threat and could be used to collect the personal data of citizens. **CNN** reports that TikTok is not the only Chinese tech giant to raise US suspicions – wireless company Huawei has earned the criticism of the Trump administration, which has campaigned worldwide against the use of Huawei equipment, citing the company's ties to Beijing. But Huawei isn't the viral phenomenon that TikTok has become, capturing millions of teens and adults with its ability to create and share short videos set to catchy music. **The two-year-old app has been downloaded over 750m times in the past year.**