KCS Group Europe

International tension and the changing face of cybercrime: predictions for 2022

December 2021

The past two pandemic-afflicted years have seen coronavirus dominate the news agenda, and what would in typical times be headline news, relegated off the front page. As the world prepares to enter the third year of uncertainty, now more than ever must the key events be treated with appropriate gravity; as they will contribute towards whatever the 'new normal' looks like. Here we present some predictions about what 2022 could look like…

<u>Russia to march into Ukraine, and get away with it</u>

While Europe is preoccupied with debating Covid policies, Russia is poised to re-invade Ukraine. With ninety-two thousand troops amassed along the border and rising reports indicating an incursion by the end of January, this is not a simple flexing exercise. This is a military deployment intended to take control of Ukraine. It is driven by the historical compulsion – Russia viewing the citizens of Ukraine as having been 'gifted' the region and not truly independent – but also for present-day, self-serving political and economic interests. Tensions have been building throughout 2021, with Ukraine trying to break ties with Russia and build new relations with Europe. Not only did Russia impose fuel sanctions on Ukraine in October when the latter refused to renew their fuel contract with Russia due to price hikes – proving that Moscow is still the predominant player in the oil & gas industry – but she supplied a list of demands to reduce tensions that was all but unacceptable from the start – not least in demanding that NATO abandon Ukraine for all time.

Russia is spoiling for a fight, and it looks like in 2022, it might get one. Further military incursion into Ukraine is all but inevitable given the rhetoric and material build-up stemming from Russia over the past year, and with NATO commitment of troops being unlikely, Russia could effectively push on into the Donetsk/Luhansk regions with little meaningful resistance. It worked in Georgia in 2008, and in the Crimea in 2014 - why not now? This might be the time that Putin finally throws down his cards – to find that the West has been bluffing with a poor hand all along.

China to maintain suppression tactics against Taiwan

On the other side of the world, China is playing the same hand regarding brinksmanship with a territory it regards as naturally hers. Taiwan has been a contentious issue since 1948 and, with increasing political and economic relevance with particular significance to the comparative situation in Hong Kong, is only going to become 'hotter'. The Chinese Foreign Minister Wang Yi, has even stated that the West is attempting to 'use Taiwan to control China'. With Chinese military victory being far from a sure thing, she is wielding economic coercion as her weapon of choice. For instance, in recent weeks alone, Lithuanian trade has been sanctioned due to Vilnius' hosting a Taiwanese Representative Office, and Nicaragua cut all diplomatic ties with Taiwan due to the need for Chinese trade being greater. Notably, Taiwan has just fourteen international allies; down from twenty-one since President Tsai Ing-wen took office in 2016. Trade and economic matters are thus weaponised – and are effective.

This 'either/or' political & economic strategy is expected to be the focal point of Chinese relations worldwide in the coming year: continuing to hold back from outright military action (yet maintaining the joint war games with Russia to enhance presence in the China Sea and irritate America, Japan and South Korea all at once) but using this economic weapon against both Taiwan and the United States. With the US sanctioning Chinese firms for human rights violations in the Xinjiang region, and Chinese war-of-words having seen no cooldown in the transition from Trump to Biden, it is unlikely that the two superpowers will lock heads militarily but in a climate of financial and political pressure, tensions will rise regardless and the range of opportunities be fewer. The temperature is only going to go up.

Ransomware to become a matter of State

The pandemic has propelled our symbiotic relationship with the digital sphere into new dimensions. The way businesses view necessity, accessibility and trust have changed – and so too have the cyber-criminal fraternity adapted and shifted their methodologies to fully exploit the vulnerabilities posed by remote working. We can expect ransomware attacks, already the most predominant form of attack, to increase in both scale and seriousness as cyber-criminals 'double down' on the new and improved methods of delivering spyware and malware via email outside of business premises' secured networks. While tightening security around remote workers' devices and networks will assist in minimising risk, nothing is ever fool-proof all the while the 'human element' remains in play.

Ransomware costs globally are expected to reach $20bn USD by the end of this year, with average individual cost being $4.24m USD – we expect both figures to rise significantly. It is discouraging that the firm responsible for managing the Police National Computer were hacked earlier this month by Russian-backed cybercriminal group 'Clop', gaining access via email backdoor and leaking sensitive data onto the dark web when the police refused to pay.

However, we expect the most significant increase to be in the degree to which states sponsor and control cyber-criminals: not only in terms of ransomware, but in the expression of propaganda, deepfakes and fake news. An economic weapon to hamstring companies in 'enemy territory', and a political weapon to control the narrative. In a world where vulnerabilities are more plentiful than ever – where your smart washing machine or car can be turned against you, or virtually anything can be presented as true – cyber will solidify its place as the new front of open warfare. Small odds perhaps, on another catastrophic hack attack against a government-related institution before 2022 is out?

The threat profile continues to adapt

In terms of direct threats to corporates, these will continue to be heightened by the pandemic and the need for businesses to recover from financial maulings over the past two years – and of how bad actors can capitalise upon this. There will likely be a rise in the deployment of cyber-competitive tactics such as website disruption, character assassination and reputational damage by those seeking to carve out a particular sector for their own and 'taking the gloves off' when it comes to setting themselves above the competition. But also, businesses are more than ever before at risk from being railroaded into taking a decision or making a deal under pressure, and at distance, and being unwilling (or unable) to let any seemingly half-decent chances disappear.

It is to be hoped that 2022 is the year in which corporates can fully embrace due diligence as a vital element of any business strategy rather than a box-ticking exercise or needless waste of money; although we suspect that at least one company will suffer a huge financial or reputational embarrassment before that happens. Not that it will ever be made public, but a new record for the number of business opportunities being controlled by Politically Exposed Persons or highly corrupt individuals would not be a surprise in the slightest.

Taking the money and running…

And finally, it would not be at all surprising if two further developments occurred in 2022: a fourth leak of sensitive offshore papers to go alongside the Paradise, Pandora and Panama Papers in revealing the dirty secrets of the rich & powerful, and the biggest fraud yet from the cryptocurrency quarter. Both of these would go some way towards exposing the outright fraud and moral corruption employed by bad actors and elites alike. The exposure of crypto as a needless gamble at best, and an obvious fraud at worst, coupled with decisive action being taken as a result of yet more undeniable indications of just how entrenched financial elitism is, would surely make 2022 a better year than its immediate predecessors by default. Perhaps it is a hope too far – but a little positivity at Christmas never hurt anyone.

KCS Group Europe

KCS Group Europe - Strategic Intelligence & Corporate Security

A leading provider of security and intelligence services, we operate discreetly in some of the world's most difficult environments on complex cases of fraud, theft, corruption, or market dynamics. We gather intelligence through the discreet use of human sources to level the playing field and help our clients identify and deal with any risks, weaknesses and threats which could impact on their business, financially or reputationally.

Our key areas of expertise include:

Corporate Intelligence Services - New market or sector entry research - Know your customer screening

In addition, through our specialist team at KCS IS, we offer a unique service in the areas of Cyber Security and Cyber Risk. This covers penetration testing, vulnerability assessments, intelligence gathering and cyber security audits - providing unparalleled analysis, contingency planning, and implementation.

To find out more or to arrange a meeting to discuss your business needs, please email the team at info@kcsgroupeurope.com or call (00 44) 207 245 1191.