KCS Group Europe

The day after the balloon went up

February 2023

Social media, intelligence services and diplomats alike are all currently poring over images (and debris) of suspected Chinese spy balloons shot down over the USA, with explanations ranging from the prosaic 'weather balloon' to 'military surveillance drone' – and it taking the White House eight days to formally rule out extra-terrestrial involvement. But while the Western world deplores China's latest display of bad altitude, it is as always at ground level where the real threat lies…

Commensurate with the rise in social media, spread of technology and the everyday informational free-for-all of the 21st century has been the weaponisation of fear. In brute force terms, you no longer needed an enemy to declare war by rolling tanks across the border or mobilising the troops, they could now strike at you from the darkest corners of the Internet – and oftentimes, never let on that it was them. Threats to key infrastructure and assets were not confined to bombing raids, suicide attacks and the like, but remote hacks and compromises that shifted 'warfare' to a low-cost, high-efficacy dynamic like never before. And most crucially, with the ability of a foe to strike anywhere, anytime, came the wave of whispering voices reinforcing the idea that they *might*.

Technology allowed for fake news and propaganda to be elevated into a full-time, global art form, and the real majesty was that oftentimes, the bad actors really did not need to do much at all: just send a few virtual balloons into the cyber stratosphere and watch the fallout. Consider how Russia seeded the 2016 Presidential election with the infamous 'fake news' and watch this develop into an armed storming of the Capitol five years later; or how China pushed misinformation to reduce the trust in Western vaccines to see swathes of European populations rebel against the very idea of science. Both of these instances, built around very specific causes, have seen the problems of misinformation and fake news explode to cover any angle of political, economic or social life one can imagine, with governments facing major challenges convincing their own people that it is not, in fact, all a conspiracy. The longest-lasting wounds are always the self-inflicted.

This is a state of affairs which particularly benefits China, Beijing playing as it always does the long game. While Russia's increasingly visible aggression led it to Ukraine and the exposure of failings across the military and political spheres that may yet prove fatal for the post-Soviet Kremlin, Beijing has always adopted the slower approach in the grains-of-sand analogy: if you must clear a beach, send one thousand people to each quietly pick up one grain, rather than (as Putin would do) use a strike team to physically rip the beach away. (Certainly the 450 million propaganda posts estimated each year by recruited civilians is indicative of this beach-clearing approach, and this does not even account for the professionalised military/agency activity). State control of domestic media outlets and the Internet (the 'Great Firewall' of China) is well known but Beijing has made manipulation of foreign thinking both an industry, and an imperative.

Aside from the question of vaccine efficacy, state-sponsored misinformation has been planted regarding the plight of Muslims in Xinjiang, a revival of Western imperialism under Biden (particularly as related to the South China Sea) and American biological weapons being discovered in Ukraine. All patently false, yet all gained traction. This is part of China's self-declared 'cyber sovereignty' strategy, namely that to dominate your people you must control all the means of information, and to do *that* means you must control all the information, everywhere, at all times. While success on the above topics would be nice, China is also simply attempting to see what works, and what it can get away with. What are the best forums and means to spread the disinformation? What level of meaningful scrutiny or pushback is there? And if you can make them believe in one thing – or at least sow the doubt – what else can you make them do?

The natural successor to simply manipulating information is to actively use cyberspace to disrupt and manipulate on a broader scale, built upon the lessons of finding out just how credulous your target audience is. Phishing emails to corporate targets chosen for their data, access or connections, who may then be the target of data theft or ransomware, are built on the same 'strategic distraction' principle as the social media propaganda wave, albeit designed to achieve a more specific and immediate response. The credulous user who clicks a phishing link or follows a fraudulent email request because their default position is to challenge nothing, or the company which inks a deal with a Politically Exposed Person because they fell for the positive propaganda designed to deify him – all water drawn from the same well. And yet, the corporate sector is still reticent to acknowledge the scale of this problem – either out of an arrogance that they know their own business best and wouldn't fall for anything, or the embarrassment that comes with admitting that they are out of their depth when dealing with it. Either path reinforces the commercial malaise, and strengthens the conviction of Beijing, Moscow and others that the truth is whatever they choose it to be.

The Head of MI6, Sir Alex Younger, has said that *'the UK must wake up…* [to being under] *the full press of Chinese espionage'*. In this he is right, but the problem goes far beyond Beijing. Even as this article was prepared, news broke of an Israeli disinformation-for-hire squad, 'Team Jorge', allegedly used by governments and corporations alike to rig elections, control the narrative and generally manipulate public opinion. All of which is an operation far more effective, and harder to combat, than sending up a balloon. So, while the truth may be out there, we do not need to look to the skies.

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, 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) 2072451191.