Great Britain: Russia hacked me. The far left smeared me. Now it’s time to fight back

Monday 18 December 2023, by MASON Paul (Date first published: 12 December 2023).

By hacking journalists, Russia is trying to stifle our democracy’s information flow

I was in my wetsuit, ready to go surfing, when I first saw evidence that my email had been hacked. I spent the next hour, still wrapped in neoprene, contacting people whose messages had been compromised. There weren’t many because – following standard journalistic practice – I use multiple encrypted accounts when I communicate with sources in politics, security and defence. But this account had been blown.

Within days it was clear that some of those sources, too, had been hacked – and not by amateurs. This was a sophisticated spear-phishing operation, whose *modus operandi* was all too familiar to the cyber specialists I turned to for help. This, they said, was likely the work of Coldriver, a hacking group linked to Russian intelligence.

Then came the “leaks” – a euphemism for material purportedly gleaned from my emails, which – I have to use legalese here – “may be a mixture of real, edited, altered and faked”. The person who published it was the former *Russia Today* and *Sputnik* journalist Kit Klarenberg – who, via an outlet called *The Grayzone*, spread the allegation that I am an “asset” for British intelligence, though he could never quite decide whether it was MI5 or MI6.

For the record, this is totally false. And though my family had a chuckle at the idea of me being some kind of Lancashire James Bond, it soon proved to be not very funny.

Klarenberg claimed to have received the material via “anonymous burner email accounts”, which means he had no idea what was real and what fake. As a result, no reputable newspaper or media group would touch the story: even right wing tabloids who hate my guts obeyed the basic principle of not using material that is unlawfully obtained and unverifiable.

Only niche outlets of the alt-left – *Novara Media*, *MintPress News* and the *Morning Star* – were prepared to give the story oxygen. The results were predictable to anyone who knows how information warfare works: random physical harassment by people who only get their news from such outlets, organised trolling on social media and attempts to “cancel” me as a member of the Labour left.

The hack, the leak, the smears and the cancellation were triggered not simply because I campaigned for solidarity with Ukraine, but because I named those spreading Russian disinformation and investigated how Russian and Chinese-aligned influence networks were targeting the British left. When I appeared as witness in a BBC investigation into academics who have peddled Vladimir Putin’s line, the BBC team was targeted, too.

I was told by those investigating the attack – which include the National Cyber Security Centre and the National Crime Agency – that they would probably be unable to attribute the attack to the Russian state, because of the very high bar of evidence needed.

But last week they did. The attacks on me, the SNP MP Stewart McDonald, the retired army officer Christopher Donnelly, the former MI6 chief Sir Richard Dearlove and scores of unnamed others, was part of an operation by the KGB's successor agency, known as FSB.

This, then, was not simply a cyber-attack: it was part of a cyber espionage campaign designed to disrupt the functioning of our democracy. And though the government has been rightly economical with the details, it's obvious to me that it was long-term and extensive.

Since before the Brexit referendum, Russian intelligence has been perpetrating a mixture of propaganda, influence, intelligence-gathering – and pressure tactics against those who stand in its way. In short, it has been conducting hybrid warfare across all parts of British democratic life: any target list that includes myself and Dearlove, an arch Brexiteer and real-life former spy chief – shows how broadly the attack was spread.

The problem with hybrid aggression is that, as with terrorism, the most effective means of resisting it can lead to erosions of the very democracy we're trying to defend.

What we can do is take precautions and fight back. Just as western executives visiting China now use disposable phones and laptops, it is sensible for all politicians and most journalists to do what I've been doing for the past 18 months: using Signal for secure comms, WhatsApp sparingly, and email for almost nothing. Two-factor authentication, biometrics on all devices, and military-grade password generators are also *de rigueur*.

The Stasi in East Germany had a word for what the FSB tried to do to me and others: *Zersetzung*, which means disrupting someone's ability to function by destroying their reputation and sabotaging their work.

By attacking journalists, academics and experts – who necessarily remain unprotected by the security systems of Whitehall and Westminster – Russia is trying to stifle the information flow on which our democracy depends. The message is, if you investigate Russia's proxies and thwart its objectives we will go after you in such a way that deters others from doing so.

Fortunately, thanks to the National Security Act 2023, whose full provisions come into force this month, the state will have better tools to deal with such attacks in future. Under the act, if you damage someone's reputation, or threaten them, or deliberately lie about them, and you do so intentionally to support an interference operation by a foreign state, you are looking at up to 10 years in jail; and 14 years if it involves electoral interference.

These powers remain untested in the courts. I look forward to them being tested.

Paul Mason

P.S.

The New European

https://www.theneweuropean.co.uk/paul-mason-russia-hacked-me-the-far-left-smeared-me-now-its-time-to-fight-back/