KCS Group Europe

Power to the people?

Russia has accused America of hacking into its power grid and planting viruses. Not for the first time – and coincidentally only a few days after much of South America was blacked out – the two old foes are stoking fears not that a new cyberwar is on the way, but that it has already begun. And it is likely that this is true – not only is the next global war likely to not be fought with tanks or nuclear bombs, but that it has already entered a sophisticated phase of sorties, attacks and surgical strikes. The language of warfare stays the same but this goes beyond even being just a cold war – in the world of state-sponsored cyber-attacks, this conflict has never been hotter.

Both the Americans and the Russians (plus, of course, most other major powers around the world) have form in this area: either using a government agency outright, or co-opting private hackers, to go after a target to either simply probe its weaknesses or launch an outright attack. Clearly, the consequences of the Russian power grid going down for any great length of time would be severe, and it would not be beyond an opposition to war-game this to understand the practical possibilities. Sometimes there is a genuine threat (as when the Shamoon virus wiped out Saudi Aramco's production capabilities. Sometimes, as with the alleged power grid strikes, there is simply a testing of the waters, or a flag saying: we were here. An indication of threat can be just as powerful as direct action.

Given Russia's direct use of the term *'cyberwar'* in threatening a response, such actions would have to be considered in the 'hard power' area of politics (which is after all itself just war by other means). Does this mean they merit an equal, if not military, response? It is a slightly grey area, not only because in the world of cyber it is not always abundantly clear just who is attacking you, but because the targets are not always appropriate to the force (we can use no other word) used. Certainly while government departments and critical infrastructure systems may be probed, the more common targets will be industrial and commercial firms: either because these are easier targets or because they have sensitive/rewarding information (cyber now being the preferred means for espionage) or, again, simply because they can. Would it be appropriate to launch a full-scale cyber attack in retaliation for one company being hacked?

For the companies caught up in this cyber-war, there can be few opportunities for restitution. Not allowed (at least under UK law) to strike back directly themselves, they are also at the mercy of a government that looks predominantly at 'the big picture' (in terms of *Us v Them* mentality rather than at the impact on individual firms) and are often unable to get their data, or their money, back. Therefore more and more resources are having to be pumped into preventing an attack to begin with, which in isolation is helpful but in reality delivers only passivity where proactivity is needed.

Cyber is also so crucial as it underpins practically every aspect of our lives. In a world where kettles have Wi-Fi connections, drones are trialled to deliver our post and where there is an app for everything, the cyber hinterland of today has arguably become the territorial land of yesterday.

If everything that encompasses 'cyber' was viewed as essentially on a war footing, and the cyber threat was as enshrined in law as physical advances are, both national governments and companies would be a lot better placed and prepared.

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 to 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 also 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 for our clients.

To find out more or to arrange a meeting to discuss your business needs, please…
email the team at info@kcsgroup.com or call (00 44) 2072451191