CYBERWARFARE:

Fighting in the Fifth Dimension

In the aftermath of the Sergei Skripal poisoning, which sent relations between the UK and Russia tumbling, the UK made clear its intention to retaliate with a cyberattack. This is emblematic of the new reality we are faced with: information-based combat has become a mainstream way to escalate geopolitical tensions and even wage war.

> *"Britain has entered a new era of warfare".*
>
> Defence Secretary, Gavin Williamson

First there was land, then sea, air and space. Now conflict has entered its fifth dimension: cyberspace. As Defence Secretary Gavin Williamson describes it, Britain has entered a "new era of warfare".

The idea that bullets and missiles can be replaced with an information-based, non-physical form of combat is an uncomfortable one. This is particularly so given that national economies, and indeed our lives, are now driven by data. The so-called 'Internet of Things' (IoT) has created a world in which we seek to have as much personal data as possible shared between the devices we rely on to make daily tasks more manageable.

This data-driven interconnectedness extends beyond household and personal devices. Data and the IoT govern everything from health databases and voting systems to physical infrastructure like nuclear power facilities and telecommunications towers.

This trend is set to continue. Data should now be thought of as infrastructure, and the next industrial revolution is going to depend on it. Early in his presidency, Barack Obama went so far as to declare America's digital infrastructure a "strategic national asset". However, like any piece of strategic infrastructure, in a conflict situation this makes it a target – one that is subject to manipulation from overseas. As the UK's National Cyber Security Centre (NCSC) has pointed out, it is a matter of "when, not if" a major attack takes place against the UK.

Understanding cyberwarfare

Put simply, cyberwarfare entails the use of information technology to disrupt the activities of a state or organisation. While the concept of a cyberwar is not a strictly defined term in international law or legal convention there are national military cyberwarfare doctrines, rules pertaining to cyberwarfare in the UN Charter, as well as applicable customary international law. In a practical sense, cyberwarfare has both offensive and defensive applications. The defensive side includes gathering intelligence, surveillance and operational preparation, whilst offensive cyber entails activity that directly manipulates, degrades, disrupts or destroys its targets.

The problem for governments and national security agencies to deal with is that the internet was never designed to be contested, let alone become a battleground of its own. Many legacy IT systems that have been installed in the UK and around the world were not designed to be resilient to this new kind of threat. Though considerable efforts have been made to improve its cyber defences, the National Health Service is often cited as a likely cyberattack target for this very reason, particularly following the weaknesses that were exposed by the WannaCry ransomware attack in 2017.

Moreover, as representatives from GCHQ stated last year when giving evidence to the parliamentary Intelligence and Security Committee, many people manufacture cheap systems and devices where they do not want to spend time and money on security. There is therefore an onus on private companies and government to work closely to buck this trend and promote implementing secure systems.

What is equally important to note about this form of warfare is that barriers to entry are relatively low. Waging cyber warfare is not like constructing a bomb or another complex piece of combat machinery – it requires the expertise, but relatively little complex capital outlay.

The UK military has thus begun recruiting IT experts as reservists. Private defence contractors also play a critical role in helping build defensive cyber capability in both the public and private sectors.

Cyberattacks

Who carries them out?

Broadly speaking, there are four categories of cyber attacker: organised criminals, who target individuals or organisations for their own financial gain; 'hacktivists', who use cyberattacks to advance a social or political cause; terrorist groups, who may seek to perform some combination of both (although they often lack the resources and expertise to do so) and; of course, nation states, who generally possess the most advanced cyber capabilities.

In almost all cases, nation states seeking to launch a cyberattack will do so by proxy. For the international community, the major headache with this is that it remains very difficult to attribute cyberattacks to specific nation states or state-sponsored organisations. Often the forensic process entails identifying a recognisable piece of code; however proving concrete state links is difficult.

What do they look like?

Perceived Russian interference in Western elections is can also be considered a form of cyberattack. It fits within Russia's kompromat ("compromising material") doctrine, which involves obtaining or forging damaging information – classified or otherwise – and releasing it via a public platform like Wikileaks or Kremlin-owned news websites, as was the case with the release of the hacked contents of the Democratic National Committee and John Podesta's emails to damage Hillary Clinton's 2016 presidential campaign.

As recent events have shown, a cyberattack can involve a threat being made to people's privacy or the economy. However, what is underestimated is the damage that can be inflicted via a cyberattack, which can also have a real-world impact. This year, the NCSC announced that it was implementing a new cyber incident prioritisation framework. The various categories of cyberattack range from Category One, in which essential UK services experience "sustained" disruption or affect national security, even to the point of loss of life; to Categories Five and Six, in which a cyberattack is carried out against a medium-sized organisation but there are indications of possible state involvement.

Since the NCSC was founded in 2016, the UK has not detected a Category One attack, so it is challenging to conceptualise how an attack could manifest itself in the UK. Internationally, the best illustration of the real-world capability of a cyberattack is the Stuxnet case.

In 2010, Iran discovered that a cyber worm or virus known as Stuxnet had been interfering with its nuclear enrichment programme for over a year without the country's knowledge. Based on photographs of the insides of enrichment facilities released by the Iranian government – then-President Ahmadinejad wanted to flaunt the country's nuclear capabilities as a show of strength – foreign hackers were able to design a malware code that reportedly interfered with the robotics in the facility and prevented the regime from developing centrifuges to enrich uranium. There is considerable evidence to suggest that the Stuxnet attack was state-sponsored although this continues to be a subject of investigation.

> *"The problem for governments and national security agencies to deal with is that the internet was never designed to be contested, let alone become a battleground of its own."*

The Political Dimension

Cases such as Stuxnet necessarily invite a more complex political discussion. However, unlike more conventional forms of combat, laws and policy frameworks governing cyberattacks are still in their infancy. Moreover, the inherently borderless nature of this form of warfare means that politics is incredibly important to consider.

Amidst heightened tensions with Russia and North Korea, policymakers have stepped up their rhetoric about the potential for the UK to fall victim to a cyberattack. In January last year, GCHQ warned the Commons Defence Select Committee about a "tidal wave" of cyber-attacks as well as the threat of a major attack in the next year. Defence Secretary Gavin Williamson has gone so far as to warn that Moscow could cause "thousands and thousands of deaths" with a cyberattack on the UK's critical infrastructure. Although this might be another manoeuvre on Williamson's part to lobby for more funding for the Armed Forces, most experts agree that a serious attack on the UK could lead to loss of life and could manifest itself in anything from jamming air traffic control systems to hacking vehicles and energy distribution hubs.

While Russia is seen as the most active power in terms of its tendency to launch state-sponsored attacks and espionage, China, Iran and North Korea are also known to possess significant offensive cyber capabilities. There are enormous geopolitical considerations involved with this given that there can be no certainty as to each country's exact cyber weaponry. All of this leads to a standoff between nations and private companies.

It must be recognised that the UK also possesses sophisticated cyberwarfare capability. In fact, when then-Defence Secretary Philip Hammond told an audience at the 2013 Conservative Party Conference that the UK was developing offensive cyber capability, it was reported to be the first time any country had openly admitted as much.

Such is the unique nature of this dimension of warfare. It is conducted more secretively than all others and yet has the power to do significant damage. No side wants to demonstrate its might for fear of unduly influencing international law or exposing itself strategically.

What comes next?

Efforts are currently underway to declare state-sponsored cyberattacks acts of war. For instance, the European Union is working on a developing a framework for its Joint EU Diplomatic Response to Malicious Cyber Activities to address the growing international cyber threat.

Moreover, the pace of technological development is going to continue, and at speeds that will create both new dangers and opportunities in cyberwarfare. The advent of innovations like artificial intelligence (AI) is a prime example, because over time it can replace the human hacker with a smarter algorithm that can perform multiple functions more quickly and more efficiently. AI-based technology is already being adopted by cybersecurity companies to root out malware and prevent attacks by constantly studying and rewriting code. The danger of course is that AI will also be used for offensive cyber capability and will be infinitely harder to stop than a human hacker. The advent of quantum computing will only compound this challenge. It is essentially a technological arms race.

Governments will ultimately need to provide a more prescriptive framework to deal with cyber issues in the context of the digital revolution.

Far from wanting to impede the pace of innovation, it is widely accepted that heightened security is going to be needed not only in critical national infrastructure but also in private firms that provide essential services across sectors such as pharmaceuticals, telecommunications and banking.

Ben Loewenstein
Director, Public Affairs
Strategic Communications,
London
+44 (0) 203 727 1324
Ben.loewenstein@fticonsulting.com

EXPERTS WITH IMPACT™

About FTI Consulting

FTI Consulting is an independent global business advisory firm dedicated to helping organisations manage change, mitigate risk and resolve disputes: financial, legal, operational, political & regulatory, reputational and transactional. FTI Consulting professionals, located in all major business centres throughout the world, work closely with clients to anticipate, illuminate and overcome complex business challenges and opportunities.

The views expressed in this article are those of the author(s) and not necessarily the views of FTI Consulting, its management, its subsidiaries, its affiliates, or its other professionals.

www.fticonsulting.com