Britain's Emerging Cyber-Strategy [1]

David J Lonsdale

ABSTRACT

In recent years, cyber power has attracted a great deal of attention in government strategy and security reviews. This has been matched by regular increases in budget and the establishment of new organisations to coordinate UK activity in cyberspace. The result is the emergence of UK cyber strategy. However, this paper argues that at present UK cyber strategy is not comprehensive, nor does it cohesively bring together the different elements of cyber power to effectively serve UK policy objectives. This article has two goals: first, to identify the components of the UK's emerging cyber-strategy; and second, to assess the UK's approach against a comprehensive cyber-strategy framework. The latter includes seven elements: defence; cyber-espionage; information manipulation; widespread disruptive attacks; raids; joint operations; and deterrence.

It was clear from *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review* (2010) that Britain regarded cyber-security as a critical issue. It was included as one of four Tier One Threats in the review.[2] With the 2015 *National Security Strategy and Strategic Defence and Security Review*, the government's commitment to cyber issues has continued. Once again, cyber-security is regarded as one of four primary security challenges facing the nation. A simple metric analysis of the document reveals the considerable attention afforded to cyber matters. The word 'cyber' appears 110 times in the 94-page document. This compares with 'Terror' or

‘Terrorism’, which appear 122 times; Russia, 28 times; and China, with 19 mentions. The government’s concern over cyber-security amounts to more than just rhetoric. Investment in cyber-security continues to grow, with new organisations being established to co-ordinate national activity. Government spending on cyber-security has almost doubled to £1.9 billion over the next five years. Later this year, the National Cyber Security Centre (NCSC) is to be established, which will bring together cyber-security expertise and act as ‘the authoritative voice on information security in the UK’. [3] In the words of Ciaran Martin, CEO of the NCSC, the new centre will ‘bring together the capabilities already developed by CESG – the Information Security arm of GCHQ – the Centre for the Protection of National Infrastructure, CERT-UK and the Centre for Cyber Assessment’. [4]

Thus, and in many respects echoing efforts in the United States, the UK is developing some of the features required for cyber-strategy. With the forthcoming release of the UK’s latest cyber-security strategy paper, this is a good time to discuss the developing subject of cyber-strategy within a UK context. In particular, it is important to establish whether the UK is developing the necessary components and doctrine for an effective cyber-strategy. In order to do this, it is first necessary to identify and collate the various components of the UK’s emerging cyber-strategy. Emergence is the correct term here, for at present the UK does not observably have a comprehensive cyber–strategy – although it has produced a cyber-security strategy, but that is not the same thing. The 2011 *The UK Cyber Security Strategy* and the 2014 *The UK Cyber Security Strategy Report on Progress and Forward Plans* are defensive in nature, and do not cover the full range of cyber-operations. [5] A comprehensive strategy would include defensive and offensive operations, and the deterrence implications of these.

Importantly, it would outline how together they serve the national security policies of the UK alongside the other instruments of grand strategy. The UK Cyber Security Strategy*,* which seeks to protect the UK's critical infrastructure and enable a secure information environment within which to do business, is a step in the right direction, but it is not enough.

In essence, this article has two objectives: first, to identify the components of the UK's emerging cyber-strategy; and second, to assess the UK's approach against a comprehensive cyber-strategy framework. The latter is constructed from the author's assessment of possible strategic actions within and through cyberspace – based on 20 years of studying cyber-operations, along with a general appreciation of the use of force across all environmental domains, whilst taking into account the unique characteristics of the cyber-domain. [6] On this basis, it is proposed that a comprehensive cyber strategy should include seven elements: defence; cyber-espionage; information manipulation; widespread disruptive attacks; raids; joint operations; and deterrence.

It is also important to establish our understanding of the cyber domain. From a strategic perspective certain features are evident. The cyber-domain is largely manmade, and is therefore constantly shifting; it facilitates the instant exercise of power (normally non-violent) on a global scale; contains the increasingly important resource of information; exists simultaneously in the virtual and physical realms;[7] and as a result of the latter occupies a legal and political grey area.[8] As the cyber-age continues to mature academics and policy-makers are still trying to make sense of the new epoch. In the field of ethics, for example, Randall R Dipert has called for the development of a ‘full ethics of cyberwarfare’.[9] In a similar vein, there is a strong need for the development of a full cyber-strategy.

The UK’s cyber-strategy stands on three pillars: defence (with resilience); offence; and deterrence. It offers increased strategic options, but suffers from some limitations and lack of detail in certain areas. In conclusion, the article advocates a more unified and comprehensive approach to UK cyber-strategy than is currently evident.

Thus far, there is no universally accepted definition of ‘cyber’..Nonetheless, it generally relates to the characteristics and culture of computers and information technology, or as the Tallinn Manual states: ‘connotes a relationship with information technology.’ [10]

The relationship between information technology and security, commonly referred to as ccyber-security, is reasonably well understood. It concerns the defence of computers, information networks and critical infrastructure from cyber-attack. Whereas, as Thomas G Mahnken notes, cyber-strategy is at an embryonic stage of development: ‘Despite sweeping pronouncements, the use of cyber means to achieve political aims remains an abstract and underdeveloped topic’. [11] An important step in developing an understanding of cyber-strategy is to provide an adequate definition. To that end, cyber-strategy can be defined as ‘the process that converts cyber-power into policy effect’. In turn, cyber-power can be defined as ‘the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power.’[12] This involves protecting one’s own cyber-assets, but also includes the offensive use of cyber-power to pursue foreign policy objectives.

Britain's Cyber-Strategy

As previously mentioned, existing UK cyber-security strategy documents from 2011 and 2014 are defensive in outlook, with only passing reference to offensive operations. Specifically, mention is made of the Defence Cyber Operations Group (DCOG), which reports to Joint Forces Command, and the Joint Cyber Unit 'whose role will be to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace.'[13] The Joint Cyber Unit sits within the Ministry of Defence's (MOD) Global Operations and Security Control Centre, which is responsible for operating and defending MoD networks.[14]

Despite mention of these units, no detail is provided on offensive operations. Indeed, the word 'offensive' does not appear at all in either document. This suggests that much of the UK's effort is aimed at defending networks and critical infrastructure, information sharing, resilience, and raising awareness and best practice in both the public and private sectors. Even though recent acknowledgement of an offensive capability suggests that this element of cyber-strategy may not be completely underdeveloped, the absence of official strategic discourse on offensive operations still merits concern. One should not assume that extant capability automatically equals strategic proficiency. US nuclear strategy during the Cold War provides some evidence of this claim. Military thinking on nuclear usage was often out of kilter with national policy, which suggests that a cohesive strategic discourse had not taken place. This could have resulted in poor, and potentially deadly strategy had nuclear war ensued. Specifically, policy-makers demanded limited nuclear options and restraint during a crisis, whereas the military wanted to go big and early to preserve assets.[15] This raises the question of whether the UK's policy-makers, intelligence agencies and military have engaged in proper strategic discourse on cyber-attack.

The UK's focus on cyber-security and defence is entirely appropriate, and well reflects the primary interests of a cyber-dependent state such as the UK. With so much of the country's economy, services and infrastructure dependent upon the reliable flow of information around networks, it is sensible to focus resources in order to detect and defeat cyber-threats. The scale of cyber-threats is well documented and therefore does not need to be outlined in detail.[16] It is worth noting, however, that GCHQ is monitoring cyber-threats from high-end adversaries against 450 companies across the aerospace, defence, energy, water, finance, transport and telecommunications sectors.[17] Furthermore, bringing together two of the major contemporary threats, in his November 2015 speech to GCHQ, then-Chancellor George Osborne spoke of the potential threat from cyber-terrorism: 'when we talk about tackling ISIL, that means tackling their cyber threat as well as the threat of their guns, bombs and knives.'[18] At present, terrorists primarily use cyberspace for recruitment and propaganda operations. There is little evidence of terrorists posing a substantial threat via cyber-attack. Nevertheless, as part of an overall campaign that includes more traditional forms of violence, offensive cyber-operations could contribute to a sense of insecurity and fulfil the 'propaganda of the deed' function of terrorist action.[19]

Since the publication of the 2011 strategy, an important shift in tone is evident. Despite the continued focus on defence, the UK is beginning to invest in cyber offensive capabilities. Announcing the establishment of a new cyber-reserve unit, in 2013 the UK government stated: ‘Britain will build a dedicated capability to counter-attack in cyberspace and, if necessary, to strike in cyberspace.’[20] The 2015 review signifies a further evolution of an offensive capability: ‘We will provide the Armed Forces with advanced offensive cyber capabilities, drawing on the National Offensive Cyber Programme which is run in partnership between the MOD and GCHQ’.[21] Then-Chancellor Osborne further highlighted this shift when he spoke of the need for increased attribution capabilities and ‘a dedicated ability to counter-attack in cyberspace.’[22] Finally, it has been reported that the UK is developing an ‘information manipulation’ capability to operate within and through social media, or what is more traditionally referred to as covert propaganda and psychological warfare. [23] Psychological operations (Psyops) have a long history of course, but cyberspace, and in particular the various forms of social media, offer new global media to operate within.

Building upon the defensive and offensive elements of Britain’s cyber-strategy is deterrence. Aping more nuanced thinking on nuclear deterrence, Britain’s cyber-deterrence is based on both denial and punishment. Denial seeks to deter an adversary by denying them the ability to achieve its goals. As Osborne notes, ‘Part of establishing deterrence will be making ourselves a difficult target, so that doing us damage in cyberspace is neither cheap nor easy.’ [24] Denial is supplemented by the threat of punishment. As is also evident in the Department of Defense Cyber Strategy, Britain seeks to link its physical and virtual means of response: ‘we are making sure that we can employ a full spectrum of actions in response.’ [25]

Denial and punishment are fairly standard concepts within deterrence. However, Britain adds a third string to its cyber-deterrence bow: developing global norms against cyber-attack. This may seem a rather ambitious and somewhat novel aspect of a deterrence posture. Nonetheless, there is already some evidence to suggest that states are increasingly displaying a degree of restraint in their cyber-actions.[26] The attacks on Estonia (2007), the Iranian nuclear programme (2009–10) and Saudi Aramco (2012) appeared to signal a rising tide of sizable cyber-attacks. However, although low-level cyber intrusions and cyber espionage continue unabated, the more disruptive and destructive forms of cyber-attack have not emerged as expected.[27] Talk of an ‘electronic Pearl Harbor’ has receded.[28] Moreover, there have been attempts within the UN and NATO (Tallinn Manual) to apply existing international law to cyber-operations in an effort to better manage cyber-relations amongst states.[29] Thus, the third element to Britain’s cyber-deterrence posture is not without merit.

A Comprehensive Cyber Strategy?

Since the UK Cyber Security Strategy lacks any substantive reference to offensive operations and deterrence – which we know from public statements are elements of Britain’s cyber-stance – it cannot be regarded as a complete statement of Britain’s strategy. Nonetheless, and as evidenced in the previous section, by combining the official strategy document, in conjunction with the 2015 defence review, various policy statements and parliamentary evidence, it is possible to construct a reasonable outline of Britain’s emerging cyber-strategy. In the absence of a clear and complete annunciation of strategy, such sources provide decent indicators of the government's position, and thus form the basis to discuss current thinking within the UK, as well as establish a baseline to assess the forthcoming cyber-security strategy paper.

As noted, within Britain's strategic cyber-posture three pillars are clearly evident: defence; offence; and deterrence. As will be discussed below, other elements are evident, but not expressed as clearly, and certainly are not evidently contained within an inclusive and coherent cyber-strategy. This article contends that all of the elements of cyber-strategy should be brought together in a comprehensive strategic approach to cyber-power. In order to assess the UK's current approach to cyber-strategy, it is important to establish what a comprehensive strategy would look like and compare Britain's approach to it.

Taking into consideration the range of possible cyber-operations and an appreciation of the use of force in general, an outline of a comprehensive cyber-strategy can be constructed. Said strategy should include seven elements: defence; cyber-espionage; information manipulation; widespread disruptive attacks; raids; joint operations; and deterrence.

Defence

It has already been established that Britain has a well-defined defensive element to its cyber-strategy. Measured against established cyber-security advice, Britain seems to have a rational and increasingly well-co-ordinated approach.[30] The defensive effort is based upon a number of different, mutually reinforcing components. These include maintaining the security of networks underpinning key services and national critical infrastructure; raising awareness and good cyber-hygiene in the public sector; improving cyber-skills; building resilience into the economic system; and establishing organisations to co-ordinate cyber-security and information sharing. [31] The latter can be seen with the establishment of the National Computer Emergency Response Team (CERT) and the forthcoming creation of the NCSC.

As in other areas, absolute security is unachievable in cyberspace. Indeed, the UK government acknowledges as much.[32] In the cyber world this is not so much a technical issue.[33] As reported in IBM's Cyber Security Intelligence Index, the vast majority (95 per cent) of security breaches are due to human error.[34] Poor cyber-hygiene includes common mistakes such as poor password practices and responding to phishing attacks, to name but two. Nonetheless, even taking into account the inherent limits of security, Britain's approach to cyber-defence appears reasonably comprehensive. With GCHQ acting as the UK's centre of cyber-expertise, the government's objectives of making 'the UK one of the most secure places in the world to do business in cyberspace' and 'to make the UK more resilient to cyber attack and better able to protect our interests in cyberspace', seem viable.[35]

Cyber-Espionage

In its traditional guise, it is entirely reasonable to regard espionage as a separate activity to strategy. Espionage is, after all, used to support policy rather than pursue it. However, there is such tactical and operational overlap between cyber-espionage and cyber-attack that the former has to be a consideration for those developing and executing cyber-strategy. As a result of this overlap, if discovered, cyber-espionage operations may be regarded as being more aggressive, more intrusive and therefore more threatening than traditional forms of espionage. Note the rising tension between the US and China over this issue. Thus far, these ‘continuous and sophisticated intelligence contests’ have not escalated to open conflict (virtual or physical).[36] However, if cyber-intrusion constitutes an aggressive act, then cyber-espionage risks breaking down the distinction between spycraft and conflict. The Tallinn Manual, for example, notes that ‘A cyber operation by a state directed against cyber infrastructure located in another state may violate the latter’s sovereignty.’ [37]

To clarify, this is not to say that cyber-espionage *per se* is an integral part of cyber-strategy. Regardless of the means used to gather data and information (cyber or otherwise), espionage is used to support policy not pursue it. However, cyber-intrusion often blurs the distinction between genuine acts of espionage and the initial stages of an attack. One act of cyber-intrusion can steal data and simultaneously insert hostile malware into a network for future acts of disruption and/or destruction.

Thus, a unified cyber-strategy has to monitor and exert some form of control over cyber-espionage activities. A state should avoid the situation in which its intelligence agencies are conducting cyber-espionage (including industrial espionage) completely removed from broader cyber-strategy considerations.

The relationship between espionage and conflict is complex, especially in the new and nebulous world of cyberspace. Thus, it may help to illustrate with an historical analogy. U2 intelligence flights over the Soviet Union were flown by military pilots, but under the control of the CIA. Thus, strictly speaking they were acts of espionage. However, their intrusive nature and military character made them rather more menacing for the Soviet Union, resulting in rising tensions between the superpowers. Both the U2 flights and cyber espionage risk(ed) blurring the line between conflict and espionage. To clarify, because the technical characteristics of a cyber-espionage operation may be indistinguishable from acts of war preparation, the victim cannot be sure of the attacker's intent. Similarly, if military units are involved in espionage (as in the U2 flights), the waters of intent are further muddied.

As is to be expected, official details on UK cyber-espionage operations are extremely limited. However, it can be at least deduced, with a reasonable degree of confidence, that Britain is engaged in cyber-espionage. First, as revealed by the Snowden leaks, GCHQ has been involved in metadata capture and surveillance under the Tempora programme.[38] Second, MI5 officially regards cyber-espionage as an extension of traditional espionage techniques.[39] Furthermore, the reports of the Intelligence and Security Committee, although subject to redaction in this area, acknowledge an increasing cyber-dimension to intelligence work, in both a defensive and offensive guise: 'The main focus of the intelligence and security Agencies' work on cyber is on countering hostile foreign Activity, covert intelligence gathering'.[40]

It is sensible to conclude that Britain should continue to take advantage of the cyber-variant of espionage, whilst being conscious of the broader implications for strategy. An overly aggressive approach in this area could prove destabilising, as cyber-intrusion becomes more of an issue amongst states. This speaks to the need for a comprehensive cyber-strategy that monitors and exerts control over all government activities in cyberspace.

Information Manipulation

It is commonly acknowledged that states and sub-state actors are increasingly making use of cyberspace to promote their causes: 'ISIL are already using the internet for hideous propaganda purposes; for radicalisation, for operational planning too.'[41] There is also evidence of states seeking to manipulate the information environment through the covert use of trolls and bloggers.[42] However, information manipulation in the cyber-age can be more aggressive. This was evident in the distributed denial of service (DDoS) attacks against Georgia in 2008 during the Russian invasion, when government websites were taken offline. As a result, the Georgian government was unable to communicate to the outside world, and as a consequence its 'side of the story' was muted. [43] In such instances, DDoS attacks are tools of information manipulation and seek to facilitate control of the infosphere.

It is entirely appropriate that the UK should seek to promote its own policy agenda through cyberspace. Radicalisation has to be confronted in the social media space, and competitor states cannot be allowed to own the information environment. Indeed, both government and internet service providers are exploring the possibilities of disruptive information campaigns in cyberspace. This is evident, for example, in Google's concept of a 'hate speech spell checker', designed to, amongst other things, disrupt terrorist propaganda.[44] However, the results of information manipulation campaigns are uncertain and cannot be relied upon to provide direct attainment of most policy objectives. In this sense, because the information environment is so dynamic and extremely competitive, it is impossible to gauge with any degree of accuracy the strategic impact of propaganda and subversion.

Take, for example, the Russo-Georgian conflict of 2008. Although novel at the time, according to Thomas Rid the impact of Russia's cyber-campaign against Georgia was minimal, its effects lasting only four days. Lucas Kello takes a somewhat broader perspective on the conflict, and concludes that the cyber-attacks impacted significantly on Georgia's ability to communicate with its own forces, as well as affecting military procurement activities.[45] Both of these perspectives provide important comment on the strategic potential of manipulating the infosphere in the cyber-age. On the one hand, Rid's analysis of cyber-information manipulation provides an important cautionary note. On the other hand, Kello's evaluation chimes strongly with the main argument of this article: that any individual component of a cyber-campaign must be integrated within a comprehensive unified cyber-strategy acting in the service of national policy. In this way, the uncertain and unquantifiable effects of information manipulation can be attached to the more measurable results of cyber-attack and cyber-operations within a joint campaign. The point to be made is that information manipulation cannot be relied upon, independently, to achieve policy objectives. However, it can play a supporting role to other operations, enhancing the impact of their effects, and indeed benefitting from the milieu of conflict.

Widespread Disruptive Attacks

Although the evidence indicates that Britain is gearing-up to conduct offensive cyber-operations, there is little detail available on what future operations may look like. This leads to consideration on the options for cyber offensive. In reality, the forms of attacks are nearly limitless. A cyber-offensive can focus on disrupting banking and financial services, energy supply, air traffic control and major industries, to name just four. Thus, to provide a manageable theory of cyber-offensive, attacks can be divided into two types, based on scale and objectives: widespread disruptive attacks; and raids.[46] This article examines both types to identify their possible roles in cyber-strategy. From the following analysis it is evident that independent cyber-offensive operations would provide Britain with increased strategic options, albeit ones that are limited in their effect.

Widespread disruptive attacks, sometimes referred to as strategic information warfare, draw on much of the thinking behind strategic bombing by air power.[47] Richard Clarke, a former White House staffer in the fields of counter-terrorism and cyber-security, predicted that cyber-war could cause such disruption as to lead to social breakdown. Even more dramatic are the views of Mike McConnell, former director of national intelligence, who compared the effects of a substantial cyber-war assault with those of a nuclear attack.[48] Whilst these statements may be hyperbolic, they do identify the objective of this form of cyber-attack: to destroy the will and/or capability of the enemy to resist. This can be achieved, in theory, by attacking key target sets within critical national infrastructures that cause a chain reaction of disruption throughout the enemy system. Alternatively, a range of critical targets can be struck simultaneously. Either way, the objective is to cause widespread disruption across the enemy's society and economy. Due to the scale of such an attack, and the potential impact on the enemy population, this offensive option is likely to be limited to large conflicts, perhaps when physical conflict is already underway.

Our opportunity to evaluate this form of cyber-strategy is limited by the fact that there have been no such attacks to date. The closest the world has come was the attack on Estonia in 2007. In a dispute over the relocation of a Soviet-era war memorial, Russian-based hackers launched sustained DDoS attacks against the Estonian public and private sectors for two weeks. Banking and government services were significantly affected for a period. However, reflecting on the scale of the attack, it is important to note that it was not designated as an armed attack, and therefore did not trigger a response under Article V of the North Atlantic Treaty.[49]

Although the attack on Estonia was limited in scale and effect, it does provide a real world example of the strategic efficacy of cyber-attacks designed to cause widespread disruption. The evidence appears to suggest that cyber-attack in this form is not an especially effective tool of strategy. Estonia did not change its policy. Considering the similarities between widespread disruptive cyber-attack and strategic bombing, this finding is not surprising. Both forms of attack rely upon the ability to erode the will and/or capability of the enemy to resist, with only the methods being different. Thus, an examination of the history of strategic bombing suggests that widespread disruptive cyber-attack will suffer from certain limitations. Like all forms of strategy, cyber-attack faces many limitations.[50] These include institutional complications, being held back by political and ethical considerations, and the substantial intelligence challenge of identifying enemy vulnerabilities in complex modern societies and economies. Most importantly, though, those on the receiving end of strategic bombing have shown remarkable resilience, both in will and capability.[51]

It is difficult to see how cyber-attack could produce more potent and lasting effects on an enemy than kinetic forms of attack. Although in theory the effects of a disruptive attack may be more widespread, it is not clear how disruption can be more coercive than inflicting death and destruction. Cyber-attacks also present the very real threat of blowback and raise legal and ethical issues concerning discrimination in targeting and effect. In sum, widespread disruptive attacks have some significant limitations as independent instruments of strategy. Accordingly, as with strategic bombing, their potential is only likely to be realised as part of a co-ordinated cyber-strategy operating in support of a broader national strategy. In these circumstances, as with strategic bombing, cyber-attack can make a contribution to the degradation of the enemy's will and capability.

Raids

Cyber-power, therefore, is perhaps better suited to more limited and more precise forms of attack with more limited objectives. These can be thought of as raids. In contrast to widespread disruptive attacks, there are at least three decent examples of cyber-raids to study: Stuxnet; Wiper; and Shamoon. The latter two may be related, in that they both involved wiping the hard drives of oil production companies. Wiper, the first of these so-called 'data-destruction' attacks, was aimed at the Iranian Ministry of Petroleum and the National Iranian Oil Company. Shamoon, which attacked Saudi Aramco, may have been a retribution attack by Iran.[52] Shamoon wiped the data of 30,000 hard drives at the oil producing company, causing massive loss of data and substantial financial losses. However, it is reported that oil production was not affected.[53] Although no substantive policy gains appear to have been achieved by Wiper and Shamoon, they do illustrate that cyber-attacks can have real impact and can be reasonably precise. From a strategic perspective, the problem for both is that they do not appear to have been incorporated into a broader cohesive strategy. Certainly, there is no evidence of follow-on or supporting attacks.

Stuxnet, the attack on the Iranian nuclear programme, can be described as a cyber-raid, designed, as it was, to take out a particular target (centrifuges) in a precision raid. Although its strategic significance is questionable, Stuxnet has had a substantial impact on the cyber-debatel. It has been variously described as an ‘absolute game changer’ and ‘a potent new form of warfare’.[54] At a technical and tactical level there is no doubt that Stuxnet represents something new. What would have taken an air strike or special operations mission in the past, with all the attendant risks and political implications, could now be done with sophisticated malware. A target can be physically destroyed via a cyber-attack. This has clear strategic significance. Stuxnet gave the US a viable attack option it would not have had otherwise.[55] Stuxnet was simply less risky, less controversial.

The novelty of Stuxnet also relates to the precision of the weapon, which could not easily have been matched by conventional means. As military ethicist George Lucas states, ‘Unless you happen to be running a large array of exactly 984 Siemens centrifuges simultaneously, you have nothing to fear from this worm.’[56] In this way, cyber-attack increases strategic options.

However, before being carried away by this new strategic dawn, some notes of caution must be sounded. As technically sophisticated as it was, Stuxnet still required human delivery into an air-gapped network. Moreover, the impact on the Iranian nuclear programme was less than impressive. According to one estimate, the attack shut down 984 centrifuges. However, the International Atomic Energy Agency (IAEA) estimates that that figure, which equates to 11.5 per cent of the extant capability, is only 1.5% higher than would be expected from normal failure rate. The IAEA also suggests that the Iranian programme was not affected because the slack was taken-up elsewhere in the system.[57] Moreover, Stuxnet was not the cheap option that many assume. It cost approximately $300 million to develop.[58] Furthermore, once it was discovered it was 'quickly and effectively disarmed.'[59] In the final analysis, it appears that Stuxnet was tactically impressive and proves that the concept of cyber-raids works. Specific targets can be successfully destroyed with precision. However, the attack had little long-term strategic significance.

Joint Operations

The above analysis demonstrates that independent cyber-attack faces a number of obstacles, yet may still have strategic utility, especially when it is incorporated into a comprehensive strategy. To further the strategic appreciation of cyber-strategy, therefore, the role of cyber-power in joint operations must be considered: situations when cyber-power acts in support of kinetic military forces. The Department of Defense Cyber Strategy has identified a clear joint role for its Cyber Mission Forces.[60] This is what Professor Sir David Omand calls, not cyber-war, but 'cyber-assisted war'.[61] As a force multiplier, cyber-attack may serve a number of purposes. The 2007 Israeli attack on the Syrian nuclear facility at Kibar offers an interesting case in point. The Syrian air defence network was hacked prior to the air assault, leaving Israeli jets a free run to their targets.[62]

Insurgents have also taken advantage of joint cyber-operations. For example, insurgents in Iraq have hacked US drone feed to confer tactical advantage.[63] In Ukraine, 'Russian cyberattacks had collapsed the communication systems of almost all Ukrainian forces that could pose a danger to the invading Russian troops.' The result of Russia's cyber-actions, as one intelligence analyst put it, is that Russia has complete information dominance in Ukraine.[64]

Such joint uses of cyber-forces enhance operations and fulfill some of the promises of the information warfare literature which for some time has been discussing the advantages to be gained from cyber-attacks against enemy networks and command and control systems.[65] In this way, cyber-operations are used to dominate the operational information environment, help to shape the battlespace and thereby provide a force multiplier effect for friendly forces. There are striking similarities to air and sea power, both of which are most effective in support of land forces in the joint environment.

Again, information on UK joint cyber-operations is limited, but there is a sense that the UK is rapidly trying to catch up with developments in this area.[66] The MoD has two principle cyber-roles: defend its own networks; and develop cyber-capabilities to enhance military operations.[67] The DCOG is part of Joint Forces Command and is responsible for delivering military effect through cyber-operations. The DCOG receives intelligence support from GCHQ and prosecutes its cyber-missions through the new Joint Cyber Unit. The Joint Cyber Unit became fully operational in March 2015 and is tasked with integrating cyber-activities across all aspects of defence operations, ensuring commanders are able to recognise the impact of cyberspace and deploy cyber-tools in the successful conduct of operations.[68]

Importantly, General Jonathan Shaw, then-Assistant Chief of Defence Staff, acknowledged that UK MoD cyber-strategy could not concentrate purely on defence. He called for the ability to go on the offensive, to manoeuvre in cyberspace. It is not entirely clear what manoeuvre would look like in the cyber-domain. We can assume it refers to the ability to outmanoeuvre the enemy, to maintain an advantage at the tactical and operational levels in cyberspace. Furthermore, reflecting a genuinely joint approach, General Shaw called for full integration of cyber-operations, noting that emphasis should be placed on the effect, not the means of delivery: '[cyber] is merely the latest medium though which to achieve effect.' [69] As a result, all operational planning now includes a cyber-dimension.[70]

With the growing importance of the cyber-domain in military operations, this all sounds encouraging. However, a Defence Select Committee report identified a lack of conceptual framework for cyber-operations and a degree of overlap between the various organisations involved.[71] The conclusion is, yet again, that there is a distinct need for a coherent cyber-strategy: a clear conceptual and doctrinal understanding of how cyber-means serve policy ends, and how this is reflected at the operational and tactical levels. This would act as the basis for a rationalisation of organisational structure in cyber-operations.

Deterrence

Deterrence, with its focus on the mind of the opponent, is a complex strategic task. Moreover, due to the challenge of proving a negative, the efficacy of a particular deterrence posture is notoriously difficult to measure. With that caveat in mind, Britain's approach to cyber-deterrence is reasonably well grounded in established deterrence theory. As indicated, British cyber-deterrence is based upon denial, punishment and establishing global norms. In its punishment form it has some parallels with NATO's Flexible Response approach of the late 1960s.[72] By combining a range of assets (both physical and virtual), Britain's response may be more credible and have a degree of escalation dominance against small to medium foes. Being able to adjust one's response, moving up or down the escalation ladder, should enhance perceptions of the certainty of response. In theory at least, Britain can escalate from virtual attack, through conventional physical response, all the way to nuclear retaliation.

The inclusion of physical response is essential, especially since it has been determined that cyber-attack may not be as devastating or effective as previously thought. Although cyber-crime and cyber-espionage continue to pose significant problems, there has been a notable shift away from talk of electronic Pearl Harbors. After years of warnings of spectacular acts of disruption, and possible destruction, the US intelligence and policy communities are increasingly talking of sustained low to medium threats.[73] Likewise, as noted in relation to the examples of Estonia, Wiper, Shamoon and Stuxnet, the empirical evidence suggests that cyber-attack is not an especially potent independent means of pursuing strategy. However, that does not mean that cyber-attack presents no security threat. An attack may fail to achieve the policy objectives that motivated it, but it can still affect the security of the target state.

That being the case, it is prudent to deter attacks if possible, through kinetic forces if required.

In this climate of reduced expectations for cyber-attack, a robust defence may prove especially effective considering the effort required for a large attack and the limited gains to be made. Conceivably, this works for raids also. Even though the investment in a raid is lower for the attacker, a low prospect of success may be sufficient to deter the attack. When it comes to cyber-defence, Britain's comprehensive approach may be enough to deter via denial. Furthermore, Britain's strong emphasis on cyber-defence may enhance the credibility of punitive attack response. Put simply, the side sporting a solid cyber-defence is better positioned to wage and survive a conflict that includes cyber-attacks, further enhancing the credibility of one's threats. In the Cold War this was known as 'warfighting for deterrence'.[74]

Finally, Britain's inclusion of global norms in its deterrence posture must be considered. There is some evidence to suggest that the more capable and active cyber-states (US, China, Russia) are becoming less aggressive in their cyber-activities, and there is a growing consensus on the need for the establishment of global norms to protect interests and stabilise cyber-relations.[75] However, relying upon such norms is questionable as the basis of deterrence.[76] Although norms have their place in managing behaviour in international politics, they are unlikely to deter everyone, especially in moments of crisis.

Of course, deterrence is not just about capability. When it comes to response, will is just as important. If Britain wishes for its cyber-deterrence posture to be taken seriously, it must be seen to be a credible actor in cyber-strategy. Potential attackers must believe that Britain will respond in the face of an attack. The evidence thus far suggests that Western responses to attack have been limited. In the face of sustained cyber-espionage and disruptive attacks by China and North Korea, the US has limited its response to diplomacy and sanctions. Likewise, NATO's cyber-deterrence posture is vague, uncertain and unconvincing.[77] Arguably, if nuclear strategy is anything to go by, Britain has not been especially good at deterrence of late. The lack of detail or talk of nuclear warfighting from successive British governments makes Britain look like a reluctant nuclear weapon state. It also suggests that Britain does not have a firm grasp on how deterrence functions. Therefore, for the purposes of deterrence (and beyond), Britain requires a more comprehensive form of cyber-strategy, one that includes a compelling warfighting discourse.

Before leaving the subject of deterrence, mention must be made of the 'attribution problem'. Cyber-deterrence, in its punishment form, is dependent upon good and timely attribution. For punishment forms of deterrence to work, the attacker must be confident that the attack can be traced back to him within a reasonable timeframe. The attribution problem poses a challenge to cyber-deterrence, so much so that the credibility of deterrence is seriously challenged in the cyber-domain. However, recent evidence suggests that the challenge is diminishing as intelligence agencies focus collection, analysis and dissemination resources on this problem.[78]

Conclusion

Britain is developing the different components required to use cyber-power in the pursuit of policy. Both defensive and offensive capabilities are emerging. Whilst the former clearly has priority, the notion of cyber-attack is becoming more evident in government discourse, investment and organisational development. Together with the establishment of global norms, defensive and offensive capabilities underpin Britain's cyber-deterrence posture. Furthermore, Britain clearly has emerging capabilities in cyber-espionage and information manipulation. There is still some way to go before Britain has a potent cyber-capability at its disposal. For example, the Defence Select Committee has expressed its concern about institutional overlap and conceptual shortcomings.[79] Nonetheless, Britain is emerging as a cyber-power.

What is currently missing from Britain's cyber-power is a comprehensive, unified cyber-strategy. In its extant form, the cyber-security strategy is too focused on defence and does not adequately outline how the various elements of cyber-strategy should function together in the pursuit of policy. Nor does it adequately explain how cyber-power interacts with the other elements of state power. A unified and comprehensive approach to strategy is required in all forms of state power. This may be even more important in relation to the cyber-domain due to the overlap between the various cyber actions. In this sense, Britain requires a clearer outline of the various cyber offensive options, how these can be used to pursue policy, and how they relate to the more defensive and less aggressive forms of cyber-power.

Some questions that may help in forming a cohesive strategy include the following. How does coercion function in cyber-attack? Are there cyber centres of gravity that can be exploited? How does cyber-warfighting function? Is cyberspace a separate domain for warfare? If so, what are its characteristics? Where does cyber-attack sit on the ladder of escalation? Is cyber-attack primarily a joint instrument or does it have independent strategic effect? Is cyber-espionage a form of attack? With the Russian actions in Georgia in mind, when does cyber information manipulation constitute an aggressive action? These are just a selection of the questions that may help stimulate strategic discourse on cyber-power.

As Britain moves the various components of a cyber-strategy into place, addressing these questions becomes ever more important. It is hoped that the answers to such questions will provide the necessary detail and depth to Britain's cyber-strategy. Although the limits of cyber-power must be borne in mind, the development of a unified and comprehensive cyber-strategy will provide Britain with a greater understanding of this new instrument, more credible deterrence and increased strategic options.

David J. Lonsdale is the Director of the Centre for Security Studies at the University of Hull. His publications include *Understanding Modern Warfare* (Cambridge, 2016), *Understanding Contemporary Strategy* (Routledge, 2012), and *The Nature of War in the Information Age: Clausewitzian Future* (Frank Cass, 2004).

Notes

[1] This research was conducted as part of the ESRC funded project, *Common Good: Ethics and Rights in Cyber Security.*

[2] HM Government, *Securing Britain in an Age of Uncertainty: The Strategic Defence and Security Review*, October 2010, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62482/strategic-defence-security-review.pdf

[3] HM Treasury, 'Chancellor's Speech to GCHQ on Cyber Security', 17 November 2015, https://www.gov.uk/government/speeches/chancellors-speech-to-gchq-on-cyber-security and Cabinet Office. 'New National Cyber Security Centre set to bring UK expertise together', https://www.gov.uk/government/news/new-national-cyber-security-centre-set-to-bring-uk-expertise-together

[4] HM Government, *Prospectus: Introducing the National Cyber Security Centre*, 2016, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/525410/ncsc_prospectus_final_version_1_0.pdf p. 3.

[5] Cabinet Office, *The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World*, November 2011, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, and Cabinet Office, *The UK Cyber Security Strategy Report on Progress and Forward Plans*, December 2014, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/386093/The_UK_Cyber_Security_Strategy_Report_on_Progress_and_Forward_Plans_-_De___.pdf, 3.2.

[6] The various uses of force are discussed in David Jordan et al, *Understanding Modern Warfare*, (Cambridge: Cambridge University Press, 2016), pp. 62-66.

[7] Mariarosaria Taddeo, 'What Ethics Has To Do With the Regulation of Cyberwarfare', *Ethics and Armed Forces*. 2014/2.

[8] The most comprehensive discussion of the legal and moral basis for cyber strategy is found in Michael N. Schmitt (ed), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge, Cambridge University Press, 2013).

[9] Randall R. Dipert, 'Distinctive Ethical Issues of Cyberwarfare', in Fritz Allhof, Adam Henschke, Bradley Jay Strawser (eds), *Binary Bullets: The Ethics of Cyberwarfare*, (Oxford, Oxford University Press, 2016).

[10] Schmitt, p. 258.

[11] Thomas G. Mahnken, 'Cyber War and Cyber Warfare', in Kristin M. Lord and Travis Sharp (eds), *America's Cyber Future: Security and Prosperity in the Information Age, Volume II* (Washington, DC., Center for a New American Security, 2011), p. 57.

[12] See Daniel T. Kuehl, 'From Cyberspace to Cyberpower: Defining the Problem', in Franklin D. Kramer, Stuart H. Starr and Larry K. Wentz (eds), *Cyberpower and National Security* (Dulles: Potomac Books, 2009), p. 38. Kuehl offers a comprehensive discussion of cyberspace and presents fourteen different definitions before providing his own: 'a global domain within the information environment whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interdependent and interconnected networks using information-communication technologies'.

[13] HM Government, *Securing Britain…*, p. 27.

[14] Yvonne Headington, 'UK MoD's Cyber Security Capabilities Questioned, http://www.battle-technology.com/exhibitions.asp?key=604

[15] Desmond Ball and Jeffrey Richelson (eds), *Strategic Nuclear Targeting*, (Ithica, NY: Cornell University Press, 1986).

[16] For a comprehensive and concise assessment of the cyber security threat see Peter W. Singer and Allan Friedman, *Cybersecurity and Cyberwar: What Everyone Needs to Know.* (Oxford: Oxford University Press, 2014).

[17] HM Treasury, 'Chancellor's Speech…

[18] ibid.

[19] This term was officially adopted at an 1881 international conference of anarchists. See Richard Jensen, "Daggers, Rifles and Dynamite: Anarchist Terrorism in Ninteenth Century Europe," *Terrorism and Political Violence*, vol. 16, no. 1 (2004).

[20] Ministry of Defence, 'New Cyber Reserve Unit Created', 29 September 2013, https://www.gov.uk/government/news/reserves-head-up-new-cyber-unit

[21] HM Government, *National Security Strategy and Strategic Defence and Security Review* 2015, November 2015, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf p. 41.

[22] HM Treasury, 'Chancellor's Speech…'.

[23] Ben Quinn, 'Revealed: the MoD's Secret Cyberwarfare Programme', *The Guardian*, 16 March 2014, http://www.theguardian.com/uk-news/2014/mar/16/mod-secret-cyberwarfare-programme

[24] HM Treasury, 'Chancellor's Speech…'.

[25] ibid.

[26] Brandon Valeriano and Ryan C. Maness, *Cyber War Versus Cyber Realities*, (Oxford: Oxford University Press, 2015).

[27] Examples of this 'cyber anxiety', as described by Singer and Friedman (p. 3), are to be found in academic writings, policy circles and the media. The following provide a brief sample of such works, and reveal that extreme concern over cyber attack has a long and continuing history: James Adams, *The Next World War: Warriors and Weapons of the New Battlefields of Cyberspace*, (London: Arrow Books, 1999); Jody R. Westby, 'Introduction', in Hamadoun I. Touré and the Permanent Monitoring Panel on Information Security (Eds.) *The Quest for Cyber Peace*. (Geneva: International Telecommunication Union & World Federation of Scientists, 2011), p. 1; Jonah Goldberg, 'Why are we Ignoring a Cyber Pearl Harbor', *LA Times*, June 16th 2015, http://www.latimes.com/opinion/op-ed/la-oe-0616-goldberg-china-cyber-hack-20150616-column.html In policy circles, Mike McConnell, the former Director of National Intelligence, compared the effects of a substantial cyberwar assault to those of a nuclear attack. Quoted in 'War in the fifth domain: Are the mouse and keyboard the new weapons of conflict?', *The Economist*, July 1st 2010, http://www.economist.com/node/16478792 The scale of anxiety is evident by the fact that in 2013 there were nearly one million online references to either a 'cyber Pearl Harbor' or a 'cyber 9/11', see Singer and Friedman, p. 37.

[28] James R. Clapper, *Statement for the Record US Cybersecurity and Policy, Senate Armed Services Committee*, Senate Armed Services Committee, 29 September 2015.

[29] See http://www.un.org/disarmament/topics/informationsecurity/ and Schmitt.

[30] Current advice on cyber security is well summarised in Singer and Friedman.

[31] For details of Britain's efforts in cyber security see Cabinet Office, *The UK Cyber Security Strategy* and Cabinet Office, *The UK Cyber Security Strategy Report.*

[32] Cabinet Office, *The UK Cyber Security Strategy Report.*

[33] For discussions on the relationship between offence and defence in cyberspace see Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica: RAND, 2009) and Singer and Friedman.

[34] Fran Howarth, 'The Role of Human Error in Successful Security Attacks', *Security Intelligence*, https://securityintelligence.com/the-role-of-human-error-in-successful-security-attacks/

[35] Cabinet Office, *The UK Cyber Security Strategy.*

[36] Jon R. Lindsay, 'The Impact of China on Cybersecurity: Fiction and Friction', *International Security*, Vol. 39, No. 3 (Winter 2014/15), p. 45.

[37] Schmitt, p. 16.

[38] Kadhim Shubber, 'A Simple Guide to GCHQ's Internet Surveillance Programme Tempora', *Wired*, 24 June 2013, http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101

[39] https://www.mi5.gov.uk/home/about-us/what-we-do/the-threats/cyber.html

[40] Intelligence and Security Committee, *Annual Report 2011–2012*, (Norwich: The Stationary Office, 2012), Intelligence and Security Committee, *Annual Report 2012–2013*, (Norwich: The Stationary Office, 2013), p. 18.

[41] HM Treasury, 'Chancellor's Speech…'.

[42] Shaun Walker, 'Salutin' Putin: Inside a Russian Troll House', *The Guardian*, 2 April 2015, http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house

[43] Thomas Rid, 'Cyberwar and Peace', *Foreign Affairs*, (November/December 2013).

[44] Dave Lee, 'Spell-check for Hate Needed, says Google's Schmidt', 7 December 2015, http://www.bbc.co.uk/news/technology-35035087

[45] Rid, *Cyberwar and Peace* and Lucas Kello, 'The meaning of the Cyber Revolution: Perils to Theory and Statecraft', *International Security* (Vol. 38, No. 2, Fall 2013), pp. 24-25.

[46] Other typologies are available. For example, Randall Dipert classifies cyber attacks as being either intrusive or unintrusive. Randall R. Dipert, "The Ethics of Cyberwarfare," *Journal of Military Ethics*, vol. 9, no. 4 (2010).

[47] For a comparative analysis of cyber attack and strategic bombing see David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004).

[48] Quoted in 'War in the Fifth Domain: Are the Mouse and Keyboard the New Weapons of Conflict?', *The Economist*, July 1st. http://www.economist.com/node/16478792.

[49] Schmitt, pp. 57-58.

[50] As noted by Clausewitz, friction is 'the only concept that more or less corresponds to the factors that distinguish real war from war on paper'. Clausewitz, Carl von. *On War*. (Princeton, NJ: Princeton University Press, 1989), p. 119.

[51] Lonsdale, pp. 164-165.

[52] Kim Zetter, 'The NSA Acknowledges What We All Feared: Iran Learns From US Cyberattacks', *Wired*, 10 February 2015, http://www.wired.com/2015/02/nsa-acknowledges-feared-iran-learns-us-cyberattacks/

[53] Jose Pagliery, 'The Inside Story of the Biggest Hack in History', *CNN Money*, 5 August 2015, http://money.cnn.com/2015/08/05/technology/aramco-hack/

[54] Mikko Hypponen quoted in Singer and Friedman, p. 118 and Lindsay quoted in Valeriano and Maness, p. 149.

[55] Authorship of the attack has now been firmly placed on the US and Israel. See Ellen Nakashima and Joby Warrick, 'Stuxnet Was Work of U.S. and Israeli Experts, Officials Say', *Washington Post*, 2 June 2012, https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html One of the most complete accounts of the development and use of Stuxnet is Kim Zetter, *Countdown to Zero Day*, (New York: Broadway Books, 2014).

[56] Quoted in Singer and Friedman, p. 119.

[57] Valeriano and Maness, pp. 153-154.

[58] ibid, p. 151.

[59]James P. Farwell & Rafal Rohozinski, 'Stuxnet and the Future of Cyber War', *Survival* (Vol. 53, No. 1, 2011), p. 27.

[60] Department of Defense, *The DOD Cyber Strategy*, April 2015, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf

[61] Quoted in House of Commons Defence Committee, *Defence and Cyber Security, Sixth Report of Session 2012-13*, December 2012, http://www.publications.parliament.uk/pa/cm201213/cmselect/cmdfence/106/106.pdf, Ev 7.

[62] Singer and Friedman, p. 127.

[63] Noah Shachtman, 'Insurgents Intercept Drone Video in King-Size Security Breach', *Wired*, 17 December 2009, http://www.wired.com/2009/12/insurgents-intercept-drone-video-in-king-sized-security-breach/

[64] James J. Coyle, 'Russia Has Complete Information Dominance in Ukraine', *Atlantic Council*, 12 May 2015, http://www.atlanticcouncil.org/blogs/new-atlanticist/russia-has-complete-informational-dominance-in-ukraine

[65] The information warfare literature has been around for some time. For an assessment of the early literature on information warfare and its implications for military operations see Lonsdale.

[66] Yvonne Headington, 'MOD's Cyber Security Capabilities', *Battlespace*, http://www.battle-technology.com/exhibitions.asp?key=604 This is acknowledged by General Shaw, quoted in House of Commons Defence Committee, Ev 15.

[67] House of Commons Defence Committee, p. 11.

[68] See House of Commons Defence Committee and Cabinet Office, *The UK Cyber Security…*, p. 26

[69] House of Commons Defence Committee, p. 21 and Ev. 9-12.

[70] ibid, Ev. 22.

[71] Ibid, p. 4.

[72] Flexible Response was official NATO strategy from 1967. As the name suggests, NATO sought to deter the Soviet Union by being able to respond to communist aggression across the spectrum of military capabilities, from limited conventional forces to large-scale nuclear response.

[73] James R. Clapper, *Statement for the Record US Cybersecurity and Policy, Senate Armed Services Committee*, Senate Armed Services Committee, 29 September 2015. This goes some way to mitigating the effects of the cyber 'hype machine',

as described in Robert M Lee & Thomas Rid, 'OMG Cyber!', *The RUSI Journal*, (Vol. 159, No. 5, 2014).

[74] Colin S. Gray, 'Warfighting for Deterrence', *Journal of Strategic Studies*, (Vol. 1, No. 1, 1984).

[75] http://www.un.org/disarmament/topics/informationsecurity/

[76] That states are becoming less aggressive in their cyber actions is a central argument of Valeriano and Maness. We can also look to the absence of a significant attack since … as an indication of a change in how states perceive the utility of cyber attack.

[77] Rid, 'OMG Cyber!', p. 9

[78] Confidence in overcoming the attribution problem is evident in the *DOD Cyber Strategy*, pp. 11-12 and Thomas Rid and Ben Buchanan, 'Attributing Cyber Attacks', *Journal of Strategic Studies* (Vol. 38, No. 1-2, 2015).

[79] House of Commons Defence Committee, p. 4.