ARI 118/2020
13 October 2020

REAL INSTITUTO
elcano
ROYAL INSTITUTE

Implications of the UK’s Russia Report for the next National Cyber Security Strategy

Danny Steed | Author, Public Speaker and Consultant | @TheSteed86

Theme

This article assesses the implications of the recent Russia Report ahead of the development of the next cyber security strategy for the UK due in 2021.

Summary

The recent Russia Report by the UK’s Intelligence and Security Committee revealed much to be surprised about in British activities against Russian Intelligence operations, most notably their areas of deliberate non-action. This article assesses the implications of these findings ahead of the development of the UK’s next National Cyber Security Strategy due in 2021.

Analysis

The long-delayed Russia Report by the UK Intelligence and Security Committee –finally released in July 2020 after originally being declared ready for publication in October 2019[1]– generated much immediate commentary on the activities of British intelligence. Most surprising however, were several areas of deliberate non-engagement by those intelligence services covered in the report. David Aaronovitch captures the essence of most reactions in stating that the face staring back at from the report ‘is not Vladimir Putin’s, it’s ours.’[2] The biggest line that most commentators shared from the report is that British intelligence “took their eye off the ball” for a variety of reasons. The true surprise from the report lies in the extent of its introspection on British activities and failings in dealing not only with the Russian threat in general, but in particular its character through increasingly sophisticated cyber operations and an open doors policy to oligarchs investing money in Britain. By revealing more about British ‘complacency, greed and self-interest’[3] the report offers an opportunity to examine the implications its findings hold for the next National Cyber Security Strategy that is due in 2021.

This article will explore the report’s findings, before analysing why these findings matter to British cyber security strategy and how the next strategy can best respond. Ultimately, if Russian interference is as the report declares ‘the new normal’ and a “whole-of-state

[1] Intelligence and Security Committee of Parliament (hereafter referred to as ISC (2020), ‘HC632: Russia’, 21/VII/2020, p. 15, http://isc.independent.gov.uk/committee-reports).

[2] David Aaronovitch (2020), ‘Complacent Britain is a soft touch for Russia’, *The Times,* 23/VII/2020, https://www.thetimes.co.uk/article/complacent-britain-is-a-soft-touch-for-russia-z6gcmrsd6

[3] *The Economist*, ‘Russian interference highlights Britain’s political failings’, 25/VII/2020, https://www.economist.com/britain/2020/07/25/russian-interference-highlights-britains-political-failings

approach"[4] is being deployed by the Russian state against not only British interests, but as part of a broader campaign to undermine the Western Liberal Order, then the next cyber security strategy must focus on far more ambitious goals than simply organisational resilience.

What the report said

In truth, the Russia report needs to be considered effectively in two parts, that which is about Russia and that which is about the UK; the former illustrates the extent and nature of the threat, whereas the latter illustrates the shortcomings in British activities and strategy. Regarding Russia itself, surprise was expressed by the ISC at noting a general lack of attention and resources, given a clear acknowledgement that Russia itself utilises a 'whole-of-state approach' in its campaign to be seen as a resurgent state power and to protect the interests of its ruling elites.

As this article focuses on aspects of cyber security, the report's findings regarding Russian expatriates and influence via financial means are beyond the scope of inquiry here. Its findings on Russian cyber activities in the support of intelligence activities are, however, of great interest. The ISC declares that Russia is a 'highly capable cyber actor' that deploys a wide array of operational methods in support of its broader strategic aims. The means given specific citation are the use of malicious cyber activity designed to influence and undermine democratic processes; the cyber pre-positioning within the Critical National Infrastructure (CNI) of other nations; phishing campaigns against a wide range of government department targets; and the leveraging of organised criminal groups to supplement its own indigenous cyber skills.[5]

The nexus between Russian state activities and organised crime has created a 'symbiotic relationship' that profoundly muddies the waters between business, corruption, and state power at the very highest levels of leadership.[6] Combined with the articulation in the report's early pages that Russia sees the UK as one of its top intelligence targets, it becomes a curious anomaly to explain the paucity of resources allocated by British intelligence in combating its threat. The gradual reduction of resources since the end of the Cold War period lends credence to the position that the UK had become complacent to a Russia that had never changed its geopolitical viewpoint or behaviour towards the UK. As Calder Walton convincingly states, London needs to accept that not only is it already engaged in a new Cold War, but that for Vladimir Putin, 'the Cold War never really ended' and the UK is following a pattern of historic strategic behaviour in underestimating Russian ambitions and ultimately reacting late.[7]

[4] ISC (2020), p. 3

[5] ISC (2020), p. 5.

[6] As stated in SIS and GCHQ oral evidence. Ibid.

[7] Calder Walton (2020), 'Britain is botching this Cold War with Russia like it did the old one', *Foreign Policy,* 29/VII/2020, https://foreignpolicy.com/2020/07/29/britain-is-botching-this-cold-war-just-like-the-last-one-russia/

The report of course redacts the latest proportion of resources that the British intelligence services devote to Russian activities, but they did release figures illustrating a significant decline of coverage over the past two decades, particularly in the case of the domestic Security Service (MI5). Twenty years ago, the report states that Hostile State Activity broadly received 20% of MI5's resources, before being reduced to 16% during 2001/02, and to 10.7% in 2003/04. This fall continued until 2008/09, when only 3% of resources were allocated;[8] the report notes that resources are now on a general upward curve, without listing precise figures. Figures are not provided at all for the Secret Intelligence Service (SIS/MI6), but are mirrored in the Government Communications Headquarters (GCHQ) in that 70% of its efforts were direct against the Soviet bloc at the height of the Cold War, dropping to 16% by the year 2000, and 4% by 2006. The primary explanation for this disparity lies of course with the allocation of resources to the terrorist threat throughout the period Jason Burke labels as the '9/11 wars.'[9] The fight against international terrorism simply devoured the bulk of intelligence resources; in 2006/07 92% of MI5's resources were counter terrorist, alongside 33% from SIS and GCHQ respectively.[10]

Based on resources alone, there is a significant disparity between the threat the UK now believes is posed by Russia and the lag in allocating sufficient resources to monitor and combat it. As the report itself bluntly states, 'On figures alone, it could be said that they took their eye off the ball', but the ISC also shows empathy for the strain placed on intelligence services that need to cover a wide arc of modern security threats ranging from supporting law enforcement and combatting organised crime, through to counter terrorism and old fashioned counter intelligence against state adversaries. Despite this empathy, the ISC is clear immediately afterward in its charge that 'reacting to the here and now is inherently inefficient' or, as this author would say, inherently un-strategic.[11]

British resources do not match the perception of threat faced by Russian activities, particularly in cyberspace. There are three key areas that relate to the future UK National Cyber Security Strategy that the report mentions: the evolution towards attribution; the question of exactly who in the state apparatus is responsible for the protection of democratic processes; and the inadequacy of current espionage legislation in dealing with threats including the digital world.

Attribution has had a long and painful history among states trying to evolve to the realities of cybercrime and cyber-attacks. Indeed, a huge incentive for the use of cyber tools as an asymmetric advantage against advanced military powers has been the shear difficulty of proving attribution to a degree that would be acceptable in international law. Conversely, it is also seen as a key incentive for powerful state actors looking to use alternative means to achieve state objectives without resorting to traditional hard power tools. The clearest case study in this latter type of cyber-attacks –that has reached near cliché status– is the Stuxnet attack on the Iranian nuclear programme, allegedly carried

[8] ISC (2020), p. 20.

[9] The "war on terror" has always been a contentious term, and this author prefers Burkes more historically nuanced label. Jason Burke (2012), *The 9/11 Wars,* London: Penguin Books.

[10] ISC (2000), p. 21.

[11] ISC (2000), p. 22

out as a joint special operation by American and Israeli intelligence services under the code name Olympic Games. Stuxnet's deployment was centrally based on exploiting the difficulty of attribution in order to retain anonymity, or paraphrase one analogy used on the programme, the best bank frauds work when the victim does not even know they have been robbed.[12]

The difficulty of attribution is however, a two-fold affair. First, has always been the technical difficulties of unveiling the methods of attack through digital forensics. Secondly is the more pressing difficulty, which is the political decision on whether or not to attribute cyber incidents. As the report states, 'the UK has historically been reticent in attributing cyber attacks'[13] but this approach is now in the middle of an evolution in Whitehall, with the committee taking the stance that the government must now 'always consider naming and shaming' as a policy. The recent history that the Committee outlines, from the condemnations of the WannaCry and Not-Petya global ransomware attacks of 2017, to the then Foreign Secretary's public announcement on 3 October 2018 in attributing a Russian GRU campaign against a wide array of targets.

While the report goes no further in its treatment of attribution, its presence and the position of the committee is significant in highlighting that the technical problems traditionally associated with attributing have been largely conquered –although they remain resource intensive. It is also important as it is a clear indication that the British political position on attribution is changing; cyber security world is heading towards a world where state actors will attribute for significant actions carried out in cyberspace. This change of position alone is worthy of much further research for its implications will be significant in state geopolitics.

Most concerning in the report, however, is the uncertainty its findings have shed on exactly who within the architecture of the British government holds responsibility for the defence of democratic processes. The influence and manipulation of democratic elections through concerted cyber campaigns of disinformation has become a key issue in the West, especially given the controversy and scale of the Mueller inquiry in America following similar concerns regarding the 2016 Presidential election.

While the UK electoral process is considered largely sound from direct attack and interference due to its distributed paper-based voting and counting system, it nonetheless remains subject to possible influence due to the migration of news and election campaigns into cyberspace itself. And although the report offers precious little evidence (beyond open source intelligence) to suggest actual interference in the 2016 Brexit referendum, it is clear in recognising that the problem of election interference and undermining of democratic processes is very real. Where the report does highlight much bigger concern is with who holds the responsibility to defend the nations' democratic processes.

[12] An alleged architect of Olympic Games paraphrased in David E. Sanger (2012), *Confront and Conceal: Obama's Secret Wars and the Surprising Use of American Power,* New York: Crown Publishers, e-Pub version, Ch. 8, p. 432.

[13] ISC (2020), p. 6.

On the view of the British intelligence services, the report states that they simply 'do not view themselves as holding primary responsibility for the active defence of the UK's democratic processes from hostile foreign interference.'[14] The consequence of this extremely cautious view was a lack of engagement in the possibility of the democratic process being subjected to foreign interference. The ISC goes as far as to say that MI5's six lines of text on the matter was indicative of such caution and that they had also not 'sought evidence' on the subject or carried out retrospective assessments to identify lessons.

The ISC is wholly correct in finding the attitude among the intelligence services in not having any role in the defence of democratic processes 'illogical' because it is a matter of defending the democratic process itself from foreign influence, not interfering or engaging with its participation. This author will go further however, to say that not only has such a position of extreme caution been illogical, it can also be argued as contradictory to the point of dereliction of duty when considered next the statutory basis on which the services operate. Specifically, as the ISC notes, the Security Service Act 1989 specifically calls for protection 'from actions intended to overthrow or undermine parliamentary democracy.'[15] Put simply, the intelligence services are already legally charged with the defence of democratic processes, the exploitation of cyber means to influence and undermine democracy is clearly a problem that has never truly been encountered before and the spies now need to catch up.

Finally, the ISC made it clear that much of the legislative basis on which British intelligence operates is now very much out of date. The Director-General of MI5 put it best in his oral evidence in saying that the powers conferred by the Official Secrets Act 1989 have become 'dusty and largely ineffective'[16] with the Law Commissions' 2017 consultation for a future Espionage Act still awaited. Most strikingly from the findings is the lack of making the act of espionage within the UK a criminal offence, comparing this to measures in the US Foreign Agents Registration Act which compels all agents of a foreign state to register with US authorities.

This among numerous other shortcomings in the current legislative arrangements, are sorely needed in order to ensure that not only does British intelligence have the operational skill to combat espionage from cyberspace and beyond, but that they also have the appropriate statutory framework to do it with. The world was a different place in 1989 and much has changed, especially regarding cyberspace [17] ; as the abovementioned *The Economist* rightly says, the 'government had better put some work into bolstering the country's defences.'

[14] ISC (2020), pp. 10-11.

[15] Section 1 (2), Security Service Act 1989, https://www.legislation.gov.uk/ukpga/1989/5/contents

[16] ISC (2020), p. 33.

[17] Kate O'Flaherty (2020), 'How the UK can get a better grip on Russian espionage', *Wired*, 25/VII/2020, https://www.wired.co.uk/article/russia-report-official-secrets-act

The future National Cyber Security Strategy

At this point, readers might be forgiven for thinking this article is far more about espionage than it is about cyber security. A bigger truth needs to be accepted by all: one cannot discuss cyber security in detail without quickly needing an understanding of espionage. The world's second oldest profession is intimately tied to cyberspace, for that is where information is both stored and shared. Operate within cyberspace the spies must, lest they find themselves rendered irrelevant. Much like the impact of cyberspace on industry and businesses, intelligence services must also adapt or die to the use of cyber tools against the security interests of the nation and the undermining of democratic processes. One key benefit to the report's delayed publication lies in its timeliness to inform the next generation of cyber security strategy in the UK, and this author will table three recommendations and a warning.

Redefine roles

The ISC labels the approach of the British government as fragmented when dealing with who's role it is to defend democratic processes, calling it a 'hot potato.'[18] Although it is an issue that crosses numerous areas and government departments, there is scope within the next cyber security strategy to help redefine the roles and expectations for a fragmented government effort in cyberspace. Defending the democratic process of course involves far more than simply the efforts of intelligence services who must also cater to other threats, but the national strategy should help alleviate the uncertainty that has been unearthed across the British government and define where each department and service plays a role.

Articulate the defence of democracy explicitly

In order to help set the expectations for intelligence services in particular, redefining roles should include the explicit declaration within the strategy that efforts are to be devoted to the defence of democratic processes as a primary objective. It has clearly been a blind spot in British intelligence coverage, and an area of concern far beyond the British Isles. The role that exploitation through cyberspace enables to influence and affect democratic processes is nascent but highly concerning. It is high time that national strategy documents declare the threats that are truly faced, rather than acting as glossy publicity documents more concerned with budgetary slicing.

At the heart of making nations a harder target[19] is establishing deterrence within the decision-making cycles of adversaries, known or otherwise. Key in deterrence has always been a clear articulation of acceptable behaviours, and unacceptable thresholds to cross alongside known responses. Simply put, deterrence is based on clarity among actors, and it is time to establish them in cyberspace. Western liberal nations have allowed the thresholds of conduct to be tested by authoritarian regimes, who have used cyber means to operate sub-military threshold campaigns against democracy itself to

[18] ISC (2020), p. 11.

[19] The phrase has been used in previous UK cyber strategies and in ISC (2020), p. 29.

attack one of the key pillars in our societies – trust.[20] Making the defence of democracy itself a key pillar of future cyber security strategies will not only send a clear message to adversaries, it will also help remove the inhibitions felt by intelligence services as has happened in Britain to proactively defend democratic processes.

Move from resilience to proactivity

The final recommendation is for cyber security strategies to address a fundamental flaw that has plagued certainly British efforts for the past half decade, which is to move to proactive measures once more. This also links to this article’s warning for the future strategy; resilience alone is no strategy at all. Resilience was of course necessary to ensure that victims of cyber-attacks could successfully survive incidents, but it is an inherently *reactive* approach that does nothing to address the systemic issues faced in cyber security. In order to build on the work achieved domestically through cyber resilience programmes, the next strategy should focus its primary efforts on addressing normative standards and international law worldwide.

To be frank, no amount of resilience can sustain constant attacks on the scale of WannaCry or Not-Petya. There is now ample cyber-attack history to demonstrate how vulnerable industry and government is, and no sensible strategy will seek to establish resilience without addressing the underlying causes of bad behaviour and cyber-attacks in the first place. Proactivity in international engagement is a must, and the next strategy should seek to establish bold policy objectives that Britain can help generate and lead among Western liberal nations in shaping a more benevolent cyberspace that is subject to the rule of law, contributing to the values and rules based international order. While active measures are needed to defend democratic processes, so too are they necessary to defend the liberal order itself.

Conclusions

In conclusion, the Russia report contains much that goes beyond solely concerns of cyber security, but so too does it include many areas of close concern to those writing the next cyber security strategy for the UK. The business of espionage and cyber security are intimately bound and will remain so for as long as network technology is key to human information, which means their place within national cyber strategies (and associated legislation) must be clearly articulated. The spies operate according to both political directives and statutory guidelines, when either of these elements are unclear or outdated, then the practice of the spies will suffer in their duty to protect the nation.

The Russia report has highlighted failings in both these areas for British intelligence, for which the blame can only lie with political leadership, not the services themselves. They face a highly capable cyber adversary in Russia, as well as new operational methodologies that continues a strategic pattern of testing thresholds by targeting

[20] Matthew Syed (2020) is right to label trust as a fulcrum of the liberal system, ‘For Russia and China, bribery is just a decoy’, *The Sunday Times*, 26/VI/2020, https://www.thetimes.co.uk/article/for-russia-and-china-bribery-is-just-a-decoy-pldl36qtn

democratic processes themselves. Any future cyber security strategy that does not redress and allay the nerves of those spies who have been hesitant to defend democratic processes will have failed to learn from the ISC's report.

The next National Cyber Security Strategy has an unparalleled opportunity to be bold. Armed with more than a decade of previous experience, a growing governmental architecture, and broader lessons such as those found in the Russia report, it is time to be creative but above all more aggressive in future strategy development. What were once hypotheticals about the uses and abuses of cyber tools to attack Western interests have gradually become clear and present dangers to our national security. The future cyber security strategy has a central role to play in establishing what the UK will stand for, what it will not accept, how to build a common shared vision for allies, and how to bolster defences against threats that now target the very foundation of liberalism itself.