Some thoughts on *The Russia Report*

Nick Must

Ahhh yes . . . the Intelligence and Security Committee of Parliament's *Russia Report*, the cushion on which the well-upholstered posterior of Prime Minister Boris Johnson sat for more than a year. I can only assume that year was required to deliberately introduce some comedic errors, because it's riddled with them.

Firstly, however, let me begin at the beginning, with a comment on the sly way that the redactions have been made to this document. In the untitled section I will call the preface, we find in the final paragraph, on page iv:

> 'The Committee believes that it is important that Parliament and the public should be able to see where information had to be redacted: redactions are clearly indicated in the report by ***.'

This is most annoying for researchers like myself who like to pore over redacted documents and use the length of the traditional black bar redaction to be able to deduce, in some cases, the very information that is supposedly being kept secret![1] Some poor soul was given the task of highlighting every redaction, of any length, in the report and replacing them with '***'. Sneaky, very sneaky.

I have already mentioned the factual errors within the report but I should also point out that it appears to be contradictory.

Paragraph 2 has this on the Russian state:

> 'By contrast, *it has a small population compared with the West*; a lack of both reliable partners and cultural influence outside the countries of the former USSR; a lack of strong public and democratic institutions, including the rule of law; and, *of course, a weak economy*. (Emphases added)

Then, paragraph 3 has this:

> 'Despite its economic weakness, *it nonetheless heavily resources its intelligence services and armed forces, which are disproportionately large and powerful*. Moreover, Russia is adept at using its apparent weaknesses to its advantage: for example, its poor national brand and lack of long-term global friends *appear to* feed its enormous risk appetite – *perhaps* on the basis that it thinks it has nothing to lose . . . .' (Emphases added)

---

[1] For an example of this, see my 'Using the UK FOIA, part II' in *Lobster* 75 at <https://www.lobster-magazine.co.uk/free/lobster75/lob75-uk-foia.pdf>.

And paragraph 4 continues in the same unassured form 'it appears'; 'seems to'; 'seemingly fed'; 'a sense that'. Then the next paragraph suddenly moves into a much more forthright gear:

> 'Russia's substantive aims, however, *are* relatively limited: *it wishes* to be seen as a resurgent "great power" – in particular, dominating the countries of the former USSR – and *to ensure* that the privileged position of its leadership clique is not damaged.'

With paragraph 6 it's back to supposition: 'It appears'; 'witnesses have suggested'; 'likely to be'. Reading such flip-flopping, I suspect the author(s) had little confidence in their source material.

But wait! It's not only confusion that is being introduced but its cousin, obfuscation, as well. Paragraph 10 claims: 'We have been told, repeatedly, that the Russian Intelligence Services[RIS] will analyse whatever we put in the public domain [i.e. the unclassified, public copy of the report]'. But there is no mention *either way* of whether RIS has the capability to also obtain the secret, classified Annex to the Report.

It is then almost comic that paragraph 12 (at the first bullet point) says 'Most surprising, perhaps, was the extent to which much of the work of the Intelligence Community is focused on ***.' when this redaction *undoubtedly* relates to terrorism.[2] Why on earth be so coy about something that is so obvious? Perhaps the reason is that the testimony given to the Committee had shown that the public's perception of the threat from terrorism[3] far outweighed the likelihood of them being personally affected by any possible such attack.[4] If so, then the core focus on terrorism is merely a sop to the public's exaggerated fear – energies that would surely be better spent reassuring the public that they are safe and that their perception is incorrect.

Another perplexingly obvious redaction comes in paragraph 13 (at the second bullet point):

> 'Russia has also undertaken cyber pre-positioning activity on other

---

[2] See, for example <https://tinyurl.com/yyjgxycv> or <https://theconversation.com/russia-report-intelligence-expert-explains-how-uk-ignored-growing-threat-142947> and <https://tinyurl.com/uaw9xve> or <https://www.thetimes.co.uk/article/terrorism-in-the-uk-number-of-suspects-tops-40-000-after-mi5-rechecks-its-list-pqm6k62ph>.

[3] See 'Terrorist attack in Britain expected by 84% of people' (from the pollsters YouGov) <https://tinyurl.com/y3abopo7> or <https://yougov.co.uk/topics/politics/articles-reports/2016/08/04/terrorist-attack-britain-expected-84-people>.

[4] See 'The Chance of Being Murdered or Injured in a Terrorist Attack in the United Kingdom', blog post from the Cato Institute, 15 August 2018 <https://tinyurl.com/y4cj7pra> or <https://www.cato.org/blog/chance-being-murdered-or-injured-terrorist-attack-united-kingdom>

> nations' Critical National Infrastructure (CNI). The National Cyber Security Centre (NCSC) has advised that there is *** Russian cyber intrusion into the UK's CNI – particularly marked in the *** sectors.'

(A footnote in the document clarifies that there are '13 CNI sectors: Chemicals, Civil Nuclear, Communications, Defence, Emergency Services, Energy, Finance, Food, Government, Health, Space, Transport and Water.') Redactions in that second bullet point must be 'significant' and 'energy'. I say this because the public domain evidence is overwhelming.

The *Daily Telegraph,* the paper of choice of the Tory Party, has four times recounted episodes where the UK's power grid was exposed to Russian hacking. We kick off with 'Russians hacked energy companies on election day, GCHQ claims' from July of 2017:

> 'Britain's energy companies were hacked on the day of the General Election by computer criminals believed to have been backed by Russia.
>
> The Government's electronic spy agency GCHQ said in an official report sent to the energy sector that companies "are likely to have been compromised" in the wake of the attack launched on June 8.' [5]

Then, on a single day in November of 2018, we had two stories. First was 'Britain needs a 50,000-strong cyber army to protect against prolific Russian hackers, warns Nato adviser', which included the startling admission that:

> 'Britain will be wide-open to state-sponsored hacking of its critical infrastructure – *including its energy supply* – for the next decade because of a shortage of 50,000 cyber-security specialists, a top Nato adviser has warned.' [6] (Emphasis added]

The second on that autumn day was 'How Russian hackers almost shut down UK's power grid on election day',[7] a rerun of the 2017 story.

Most recently, earlier this year, *The Telegraph* reported how Elexon, 'a key player in the energy market between power station operators and firms that supply households and businesses', had been the victim of a cyberattack that had affected its 'internal systems and company laptops' (although it 'declined

---

[5] See <https://tinyurl.com/y6fccofk> or <https://www.telegraph.co.uk/news/2017/07/18/russians-hacked-energy-companies-election-day-gchq-claims/>.

[6] See <https://tinyurl.com/y2onxrcg> or <https://www.telegraph.co.uk/technology/2018/11/03/shortage-50000-cyber-security-specialists-leaves-britains-power/>.

[7] See <https://tinyurl.com/y924s7re> or <https://www.telegraph.co.uk/technology/2018/11/03/russian-hackers-able-break-uk-power-companies/>.

to give further details').[8] This lack of information was not a problem though because, the very next day, *Forbes* felt it was able to give us the griff with 'Cyber Attack On U.K. Electricity Market Confirmed: National Grid Investigates':

> 'The company that facilitates payments on the U.K. electricity market, tracking the trade between those who produce electricity and those who supply it and resolving the differences, has fallen victim to a cyber-attack. Elexon is at the center of the balancing and settlement system, working with Great Britain's National Grid Electricity System Operator (ESO) to keep the lights on. The lights didn't go off across the U.K. as a result of this cyber-attack, but internal IT systems and laptops at Elexon went dark.' [9]

Even the UK government's own *'Public Summary of Sector Security and Resilience Plans'*[10] (from 2017) details how virtually every sector within the CNI is vulnerable to knock-on disruption if the power supply grid is lost or severely disrupted.

> 'Communications Sector' – 'telecommunications, internet, postal services and broadcast' – 'Major risks to the sector include *disruption to energy . . . .*'
>
> 'Defence Sector' – 'Defence has a number of dependencies, including *power supplies*, telecoms and key personnel.'
>
> 'Emergency Services Sector' – 'Police, Ambulance, Fire and Rescue, and Maritime and HM Coastguard' – 'The major risks to the sector are loss of communications and *loss of power.'*
>
> 'Finance Sector' – 'There is also a potential impact on the finance sector from *disruption to other sectors such as energy* and telecoms.'
>
> 'Food Sector' – 'there is recognised dependency on other critical services such as fuel, *energy*, transport and communications.'
>
> 'Health Sector – 'Department of Health will be working across the health sector to consider resilience to *prolonged electricity supply disruption* and

---

[8] See 'Key part of electricity network hit by cyber attack', 14 May 2020 <https://tinyurl.com/y4xvt79o> or <https://www.telegraph.co.uk/business/2020/05/14/key-part-electricity-network-hit-cyber-attack/>.

[9] See <https://tinyurl.com/y9xgtaww> or <https://www.forbes.com/sites/daveywinder/2020/05/15/cyber-attack-on-uk-electricity-market-confirmed-national-grid-investigates/>.

[10] < https://tinyurl.com/y67kfzgm> or <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/678927/Public_Summary_of_Sector_Security_and_Resilience_Plans_2017__FINAL_pdf___002_.pdf>

fuel shortages . . . .'

'Water Sector' – 'However, *disruption to electricity supplies . . .* could result in the loss of mains water and affect the movement and treatment of sewage.' [11] (All emphases in the above quotes are added.)

Things start to get a bit weird at paragraph 20, which gives wildly incorrect dates for what were two significant ransomware attacks, labelling them 'the November 2017 WannaCry attack' – which actually took place on 12 May 2017, famously affecting NHS trusts in the UK[12] - and the 'February 2018 NotPetya attack' – which actually occurred in late June 2017.[13] Perhaps the government's document editors were too busy with all the redactions to properly fact check this information?

There is then some truly odd obfuscation at Paragraph 57, which says that 'a number of critics of Putin and the Russian government have sought sanctuary in the UK, fearing politically motivated criminal charges and harassment' and the ensuing footnote says 'These include such high-profile figures as ***.' Why redact this identity when it has to be Boris Berezovsky – the precise cause of whose death is still not resolved?

Mr Berezovsky had claimed there had already been two Russian-backed death plots against him before he finally succumbed in questionable circumstances in 2013. Perhaps the ISC received testimony from British intelligence agencies that included evidence about a link to Putin, as many have alleged?[14] Journalists from Buzzfeed news spent two years investigating fourteen (!) suspected killings on UK soil that, the investigation showed, were carried out at the behest of the Russian

---

[11] An interesting aside is provided by a report on *Zdnet* that shows how cyber-security companies create 'a distorted view of the actual cyber threat landscape that later influences policy-makers and academic work' by underplaying the threat to civil infrastructure because, as the report's title said, 'Most cyber-security reports only focus on the cool threats'. See <https://www.zdnet.com/article/most-cyber-security-reports-only-focus-on-the-cool-threats/>

[12] The government can't claim to be completely ignorant of the facts because both the NHS England and National Audit Office reports on the event got the date right. See <https://tinyurl.com/yafnoqba> or <https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf> and <https://www.nao.org.uk/report/investigation-wannacry-cyber-attack-and-the-nhs/>.

[13] See 'The Untold Story of NotPetya, the Most Devastating Cyberattack in History', by Andy Greenberg for *Wired* magazine at <https://tinyurl.com/y3o3pxq8> or <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>.

[14] Once again, the Tory's paper of choice was trenchant on the subject: 'Boris Berezovsky: "My friend Boris would not have taken his own life"' (31 March 2013) <https://tinyurl.com/y69zybha> or <https://www.telegraph.co.uk/news/uknews/9962460/Boris-Berezovsky-My-friend-Boris-would-not-have-taken-his-own-life.html>.

government.[15]

Paragraph 61 appears to show that work to combat these kind of assassinations has been hampered by a recurrence of the traditional turf war between MI5 and MI6. (The same turf war that blighted intelligence operations in Northern Ireland for many years).

> 'We welcomed this process, but questioned whether the Intelligence Community has a clear picture of how many Russians there are in the UK who are at risk – for example, would MI5 or any other relevant agency ***? This would appear to be an immediate and obvious way in to the issue, and the ***, so it would appear manageable. In response we were told that ***.'

While I have been unable to work out what has been redacted here, it would not be outlandish to suggest that the original may well be something along the lines of:

> '. . . for example, would MI5 or any other relevant agency based in the UK know of threats that originated from outside the UK, which would more traditionally be the reserve of MI6?'

– and –

> 'In response we were told that, as far as MI6 were concerned, crimes committed on UK soil were strictly the responsibility of the Special Branch and/or MI5.'

The Committee, one might assume, dutifully wanted to save the nation from seeing the children arguing in public! Paragraphs 63-77 do show, however, that MI6 clearly has the upper hand within the intelligence community. This is the section, headed 'Allocation of Effort', that details the reduction in allocation of resources to the Russian threat and the 'pivot' towards counter-terrorism. What is fascinating here is that *all* of the historical budgetary details for MI6 are redacted, when they aren't for any of the other agencies.

At paragraph 83 we get down to the real political nitty gritty, when it is pointed out that, incongruously:

> 'Policy responsibility for Hostile State Activity sits in the National Security Secretariat in the Cabinet Office. This appears unusual: the Home Office might seem a more natural home for it . . . . We understand that Government's view is that Hostile State Activity is a cross-cutting threat

---

[15] See <https://tinyurl.com/yb594fg3> or <https://www.buzzfeed.com/heidiblake/from-russia-with-blood-14-suspected-hits-on-british-soil> and the book that came from the investigation, Heidi Blake, *From Russia with Blood: Putin's Ruthless Killing Campaign and Secret War on the West* (London: Mulholland Books, 2019).

and therefore it makes sense for the Cabinet Office to hold responsibility . . . .'

Perhaps one reason it has been decided that this responsibility should lie with the Cabinet Office and not the Home Office is that, as what is effectively the 'About Us' webpage of the Cabinet Office says: 'We support the Prime Minister and ensure the effective running of government.'[16] In contrast, the same page for the Home Office venerates how: 'The first duty of the government is to keep citizens safe and the country secure. The Home Office has been at the front line of this endeavour since 1782.' [17]

Under the government of Boris Johnson it has certainly become true that supporting the Prime Minister and keeping the country safe are two completely different tasks.

As the report gets close to triple figures in paragraphs, one of the best jokes is wheeled out. Paragraph 90 covers how the intel agencies view *their own* performance – they're given the change to grade their own work, no less! The committee asked them 'to assess their current performance against the strategic objectives and plans in place in relation to the Russian threat'. The testimony from MI6 declared, *'the question of performance management and metrication . . . this is a process which is in evolution'*. (Emphasis in the original.) That from an organisation which is 111 years old and has had, for 103 of those years, the 'threat' from USSR/Russia as a major target.

At the end of the report come the inevitable credits – the list of witnesses, many of them anonymised as 'Other officials'. Blink during this and you'll miss an item of genuine interest. Listed as the lead witness from Defence Intelligence, is Lt Gen. Jim Hockenhull OBE. As a junior officer in the Intelligence Corps, Captain Hockenhull (as he then was) served with distinction in the Joint Support Group (Northern Ireland) – the 'Army Source Handling Unit' whose 'sole function was to run covert agents within terrorist organisations in Northern Ireland'.[18] Hockenhull's positions within JSG were as 'Detachment [Commander] and then Company Commander and finally as Commanding Officer'.[19]

---

[16] See <https://www.gov.uk/government/organisations/cabinet-office>.

[17] See <https://www.gov.uk/government/organisations/home-office>.

[18] See para. 5.168 (bottom of page 109) of Lord Maclean's report following the Billy Wright Inquiry <https://cain.ulster.ac.uk/issues/collusion/docs/wright_140910.pdf>. The Joint Support Group (Northern Ireland) was the renamed replacement for the infamous 'Force Research Unit' that ran agents Brian Nelson (aka Agent 6137) in the UDA and Freddie Scappaticci (aka 'Stakeknife') in the IRA.

[19] Details of this posting are given at <https://dgi.wbresearch.com/speakers/2019>.