GlobalResearch
Center for Research on Globalization

Britain's Prime Minister and the Huawei Scandal

By True Publica
Global Research, May 06, 2019
TruePublica

Region: Asia, Europe
Theme: Intelligence

Last Wednesday, Senior U.K. Cabinet ministers were hauled before a leak inquiry to determine who was responsible for the unprecedented reporting of highly secret discussions concerning national security.

Gavin Williamson was found to be guilty by an investigation of **Theresa May**'s instigation. Her letter to Williamson was not unambiguous – it categorically stated he was guilty. There was no margin for misunderstanding. As Williamson heads to the backbenches, May has made a new enemy – one who was a party whip – with all the secrets that role comes with.

But as Politico reported just a few days ago, there's more to this story than a simple leak – even if it was about national security.

> "There is another potentially culpable: former Conservative Prime Minister David Cameron. Through reforms that he institutionalized, Cameron has inadvertently brought the American political culture of leaking highly classified information into British politics. Britain's NSC is the "holy of holies." Attended by a small core of politicians and the heads of the intelligence, security and military services, it is the ultimate decision-making forum in Britain's national security architecture."

That is why I commissioned the Cabinet Secretary to establish an investigation into the unprecedented leak from the NSC meeting last week, and why I expected everyone connected to it – Ministers and officials alike – to comply with it fully. You undertook to do so.

I am therefore concerned by the manner in which you have engaged with this investigation. It has been conducted fairly, with the full co-operation of other NSC attendees. They have all answered questions, engaged properly, provided as much information as possible to assist with the investigation, and encouraged their staff to do the same. Your conduct has not been of the same standard as others'.

In our meeting this evening, I put to you the latest information from the investigation, which provides compelling evidence suggesting your responsibility for the unauthorised disclosure. No other, credible version of events to explain this leak has been identified.

It's also a little-remarked fact that, unlike many British arrangements, the NSC is a relatively recent innovation, for which Cameron is responsible. Cameron argued in 2010 that Britain needed to formalize its national security decision-making after the freewheeling "sofa government" of Labour's **Tony Blair**.

By appointing a national security adviser and instituting the NSC, partially modelled on the U.S. equivalent, Cameron gave structure to what had previously been the province of informal groups largely composed of officials. By instituting a formal entity of which he was the chair (of course), Cameron not only increased the power of the prime minister's office in the process but brought senior Cabinet ministers into the heart of national security policymaking, giving them access to sensitive intelligence, therefore significantly raising the prospect of leaks.

The National Security Council (NSC) discussed the role of Chinese telecoms giant Huawei in Britain's future 5G telecoms network and concluded some months ago that the Chinese company should be allowed to be involved. As for the mainstream media, the leak and end of Williamson's role, that is the end of the story.

However, there is more information about this story that is worthy of note. These dots may or may not be connected, the point being, there's more to understand about the motivation of Williamson's demise.

Dot One. Since stepping down as PM after the Brexit result in 2016, David Cameron now has the role of putting together a $1bn investment fund between Britain and China. The idea was to formalise a closer working relationship between the two countries. The fund was formally approved of by both Westminster and Beijing.

Dot two. Back in 2011, former government Chief Information Officer John Suffolk joined China-based IT company Huawei as global head of cybersecurity. Read those words again – former Tory government Chief Information Officer now works for Huawei as head of global cybersecurity. Suffolk was the most senior civil servant to have access to sensitive matters of government, particularly as he was also head of security risk. It was Cameron who gave Suffolk his blessing to join Huawei.

This should not have happened. It is simply too sensitive a role for someone at the heart of government and the civil service to be loyal to a foreign state business with access to the most sensitive information regarding Britain's cybersecurity. At the time, a Cabinet Office spokesman was keen to add that an "unprecedented number of conditions" were attached to Suffolk's appointment – as if that means anything in today's ruthless geo-political cybersecurity environment.

In the meantime, Suffolk has been defending Huawei to the hilt who said about the cybersecurity risk to Britain just two weeks ago that – "There's no such thing as a zero-risk connected business."

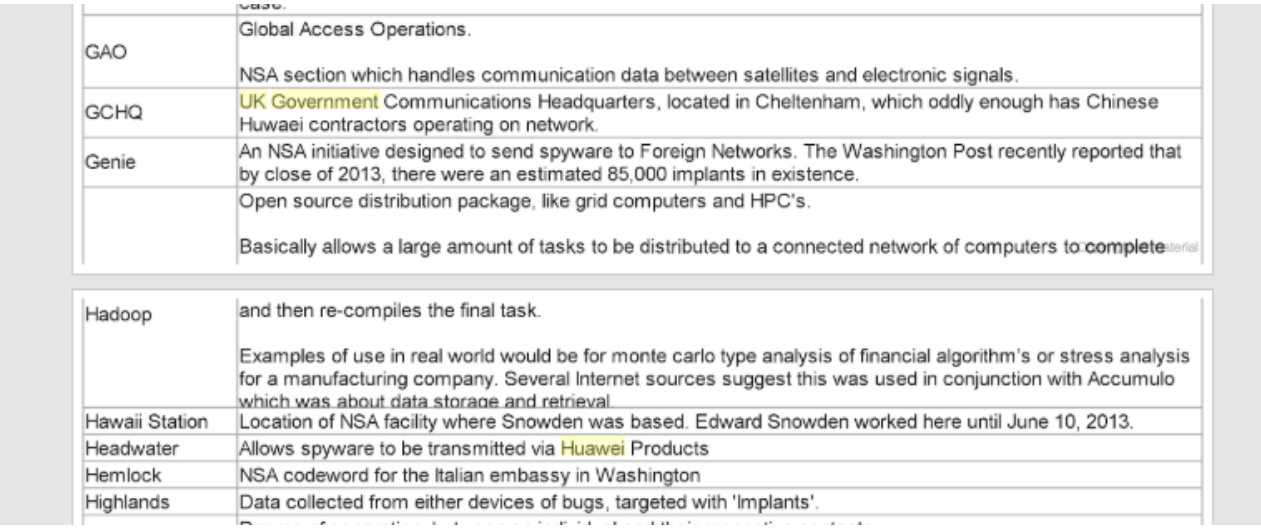
Dot three. Some months earlier in 2011, Sir Andrew Cahn stepped down after five years in charge of UK Trade & Investment, the government department that promotes exports and attracts foreign direct investment. He is currently a non-executive director of Nomura. Sir Cahn also just happens to be the Chairman of the UK Advisory Board of Huawei – a very 'comfy' connection between Huawei and the British government.

Dot four. Despite concerns about Huawei that included America forcing other 'five-eyes' nations to abandon plans to allow Huawei access to critical infrastructure projects, the UK decided to forge on ahead with Huawei. However, a recent government report concluded that Huawei's "basic engineering competence and cybersecurity hygiene was poor, which could be exploited further down the line." It went further – the HCSEC (Huawei Cyber

Security Evaluation Centre) continued to find serious vulnerabilities in the Huawei products examined. Several hundred vulnerabilities and issues were reported to inform their risk and remediation in 2018. Some vulnerabilities identified in previous versions of products continue to exist."

Dot Five: In 2012, TechRadar magazine spoke to Derek Smith, a spokesperson for the Cabinet Office, who explained that the UK government has no concerns about Huawei at all. Since then Smith has become part of the National Security Council [NSC] Head of Counter-Terrorism, Security &Intelligence Communications. He was David Cameron's Senior Press Officer on foreign policy and defence and was promoted to his current role by Cameron. Smith also disclosed in that interview – "The long-standing relationship the UK government has with Huawei, and the continued work between the two parties, means the Cabinet Office is confident that there are no security concerns."

Dot Six: In 2009, America's spy agency the NSA hacked into the Huawei router network in a programme called 'Shotgiant' which was unearthed by the Edward Snowden revelations in 2013. The project was designed to spy on the Chinese government and other companies there. In the end, the NSA was itself trying to find out how it "could exploit the equipment to spy on end users." Britain's GCHQ was involved. At the time, BT routers in the UK extensively used Huawei products and Britain's GCHQ set up a special facility for testing Huawei equipment to make sure it wasn't quietly offering access of some kind to Chinese spies and hackers. Unbelievably, GCHQ was found to have allowed "The Cell" to be staffed by Huawei employees!



GAO	Global Access Operations. NSA section which handles communication data between satellites and electronic signals.
GCHQ	UK Government Communications Headquarters, located in Cheltenham, which oddly enough has Chinese Huwaei contractors operating on network.
Genie	An NSA initiative designed to send spyware to Foreign Networks. The Washington Post recently reported that by close of 2013, there were an estimated 85,000 implants in existence.
	Open source distribution package, like grid computers and HPC's. Basically allows a large amount of tasks to be distributed to a connected network of computers to complete
Hadoop	and then re-compiles the final task. Examples of use in real world would be for monte carlo type analysis of financial algorithm's or stress analysis for a manufacturing company. Several Internet sources suggest this was used in conjunction with Accumulo which was about data storage and retrieval.
Hawaii Station	Location of NSA facility where Snowden was based. Edward Snowden worked here until June 10, 2013.
Headwater	Allows spyware to be transmitted via Huawei Products
Hemlock	NSA codeword for the Italian embassy in Washington
Highlands	Data collected from either devices of bugs, targeted with 'Implants'.

Dot Seven: The UK's recent implementation of the so-called 'porn-block' was a contract that was originally given to Huawei, which would have allowed it to control the "Homesafe" filter, which David Cameron praised back in 2013 during his push for tighter controls on adult content. The BBC discovered that UK-based Huawei employees were able to decide which sites were blocked on the service and that even users who opted out of Homesafe would have their internet usage data routed through Huawei's system. Even if that system is now served by another company, the point is that the government wants access to the information of who is accessing porn.

Dot Eight – In the 2013 Edward Snowden leaks, it was revealed that the British security services GCHQ in Cheltenham had Huawei constractors working on its networks (Image above). The file wording stated – "oddly enough, has Chinese Huawei contractors operating on their networks."

Dot Nine: A senior Conservative politician has emerged as one of Huawei's leading advocates in Brussels. Some dodgy dealings have recently emerged including hiding payments made by Beijing for many business class trips and luxury hotel stays along with 'subsidence' payments.

Conclusion

The point about these individual bits of information is this. The mix of ex-senior ministers, members of the national security council, counter-terrorism officers, GCHQ, America's NSA, senior members of Britain's 'establishment' with deep connections into the Huawei top brass, including David Cameron himself who is currently promoting a Beijing/UK trade collaboration and MEP's being bought off all sounds very 'muddy waters' when considering the nature of Theresa May's motivations for Williamson's sacking. We must also consider that British spooks have been working very closely with Huawei and their employees.

Williamson has strenuously denied the leak. He has encouraged on multiple occasions a police investigation. He has even sworn on his children's lives he is innocent – a genuinely suicidal thing to say from a career point of view if caught lying.

You don't have to like Williamson to defend him. This whole matter which has elements of the government, unaccountable security services, the decidedly murky world of geopolitical cyberwarfare and the current political conflict that Britain finds itself in – smacks of something other than we have been told. Is Williamson simply a convenient 'patsy' to demonstrate Theresa May's fortitude and power at a crucial time or is there something more insidious going on?

If Williamson is guilty of serious breaches of national security, the argument that the law has not been broken is nonsense. That is the sole reason he has been fired. Why has he not been thrown out from politics completely given the seriousness of the crime? Surely, if he was guilty of breaching national security as defence secretary he would be charged or silenced, not put back on the benches. Why has Theresa May repeatedly refused to release a copy of the findings of their investigation to Williamson himself?

There's more to this than we've been told.

And why would anyone believe Theresa May?

*

Note to readers: please click the share buttons below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

All images in this article are from TP

Become a Member of Global Research

Articles by: **True Publica**