GlobalResearch
Center for Research on Globalization

UK Sets Up Yet Another Costly Spy Agency

By Annie Machon
Global Research, November 08, 2018
TruePublica 7 November 2018

Region: Europe
Theme: Intelligence

The UK Ministry of Defence announced on 21 September the establishment of yet another British spy agency, an amalgam of military and security service professionals designed to wage cyberwar against terrorists, Russia and organised crime. The new agency will have upwards of 2000 staff (the size MI5 was when I worked there in the 1990s, not so inconsiderable). I have been asked for a number of interviews about this and here are my thoughts in long form.

The UK already has a plethora of spy agencies:

- MI5 – the UK domestic Security Service, largely countering terrorism and espionage;
- MI6 – the Secret Intelligence Service, tasked with gaining intelligence abroad;
- GCHQ – the government electronic surveillance agency and best buds with the US NSA;
- National Cyber Security Centre – an offshoot that protects the UK against cyber attacks, both state and criminal;
- NCA – the National Crime Agency, mainly investigating organised crime;
- not to mention the police and Customs capabilities.

To provide American context, MI6 equates to the CIA, GCHQ and the NCSC equate to the NSA, and the NCA to the FBI. Which rather begs the question of where exactly MI5 fits into the modern scheme – or is it just an anachronistic and undemocratic throw-back, a typically British historical muddle, or perhaps the UK's very own Stasi?

So why the new and expensive agency at a time of national financial uncertainty?

Of course, I acknowledge the fact that the UK deserves to retain a comprehensive and impressive defence capability, provided it is used for that purpose rather than illegal, needless wars based on spurious political reasons that cost innocent lives. Every country has the right and the need to protect itself, and the cybers are the newly-defined battle lines.

Moreover, it might be overly simplistic to suggest that this is just more empire-building on the part of the thrusting and ambitious young Secretary of State for Defence, Gavin Williamson. Perhaps he really does believe that the UK military needs augmenting after years of cuts, as the former Deputy Chairman of the UK Conservative Party and er, well-known military expert, Lord Ashcroft, wrote in the *Daily Mail*. But why a whole new intelligence agency at huge cost? Surely all the existing agencies should already be able to provide adequate defence?

Additionally, by singling out Russia as the hostile, aggressor state, when for years the West has also been bewailing Chinese/Iranian/North Korean et al hacking, smacks to me of political opportunism in the wake of "Russiagate", the Skripals, and Russia's successful intervention in Syria.

Those of a cynical bent among us might see this as politically expedient to create the eternal Emmanuel Goldstein enemy to justify the ever-metastasising military-security complex. But, hey, that is a big tranche of the British, and potentially the post-Brexit, British economy.

The UK intelligence agencies are there to protect "national security and the economic well-being of the state". So I do have some fundamental ethical and security concerns based on recent Western history. If the new organisation is to go on the cyber *offensive* what, precisely does that mean – war, unforeseen blowback, or what?

If we go by what the USA has been exposed as doing over the last couple of decades, partly from NSA whistleblowers including Bill Binney, Tom Drake and Edward Snowden, and partly from CIA and NSA leaks into the public domain, a cyber offensive capability involves stockpiling zero-day hacks, back doors built into the internet monopolies, weaponised malware such as STUXNET (now out there, mutating in the wild), and the egregious breaking of national laws and international protocols.

To discuss these points in reverse order: among so many other revelations, in 2013 Edward Snowden revealed that GCHQ had cracked Belgacom, the Belgian national telecommunications network – that of an ally; he also revealed that the USA had spied on the German Chancellor's private phone, as well as many other German officials and journalists; that GCHQ had been prostituting itself to the NSA to do dirty work on its behalf in return for $100 million; and that most big internet companies had colluded with allowing the NSA access to their networks via a programme called PRISM. Only last month, the EU also accused the UK of hacking the Brexit negotiations.

Last year Wikileaks reported on the Vault 7 disclosures – a cache of CIA cyberweapons it had been stockpiling. It is worth reading what Wikileaks had to say about this, analysing the full horror of how vulnerable such a stockpile makes "we, the people", vulnerable to criminal hacking.

Also, two years ago a huge tranche of similarly hoarded NSA weapons was acquired by a criminal organisation called the Shadow Brokers, who initially tried to sell them on the dark web to the highest bidder but then released them into the wild. The catastrophic crash of NHS computers in the UK last year was because one of these cyber weapons, Wannacry, fell into the wrong criminal hands. How much more is out there, available to criminals and terrorists?

The last two examples will, I hope, expose just how vulnerable such caches of cyber weapons and vulnerabilities can be if not properly secured. And, as we have seen, even the most secret of organisations cannot guarantee this. To use the American vernacular, they can come back and bite you in the ass.

And the earlier NSA whistleblowers, including Bill Binney and Tom Drake, exposed just how easy it is for the spooks to manipulate national law to suit their own agenda, with warrant-less wiretapping, breaches of the US constitution, and massive and needless overspend on

predatory snooping systems such as TRAILBLAZER.

Indeed, we had the same thing in the UK when Theresa May succeeded in finally ramming through the invidious Investigatory Powers Act (IPA 2016). When she presented it to parliament as Home Secretary, she implied that it was legalising what GCHQ has previously been doing illegally since 2001, and extend their powers to include bulk metadata hacking, bulk dataset hacking and bulk hacking of all our computers and phones, all without meaningful government oversight.

Other countries such as Russia and China have passed similar surveillance legislation, claiming as a precedent the UK's IPA as justification for what are claimed by the West to be egregious privacy crackdowns.

The remit of the UK spooks is to protect "national security" (whatever that means, as we still await a legal definition) and the economic well-being of the state. I have said this many times over the years – the UK intelligence community is already the most legally protected and least accountable of that of any other Western democracy. So, with all these agencies and all these draconian laws already at their disposal, I am somewhat perplexed about the perceived need for yet another costly intelligence organisation to go on the offensive. What do they want? Outright war?

*

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

Annie Machon is a former intelligence officer for MI5, the UK Security Service, who resigned in the late 1990s to help blow the whistle on the spies' incompetence and crimes. She has a rare perspective both on the inner workings of governments, intelligence agencies, the media, and digital rights, as well as the wider implications for the need for increased openness and accountability in both public and private sectors.

Featured image is from TruePublica.

Articles by: Annie Machon