Chapter 5

5 Beyond signals intelligence: Offensive capabilities

5.1 Introduction

Documents released by German magazine Der Spiegel provide a much richer picture of the offensive activities of the NSA and its allies, including the UK's GCHQ.[i]

The global surveillance infrastructure and hacking tools described in the previous chapters are not only used for obtaining information to be fed into intelligence reports and tracking terrorists.

The agencies are also developing cyber-warfare capabilities, with the NSA taking the lead within the US armed forces. This militarisation of the internet saw U.S. intelligence services carried out 231 offensive cyber-operations in 2011[ii]. The UK's National Strategic Defence and Security Review from 2010 made hostile attacks upon UK cyberspace a major priority[iii]. It is fair to assume that many countries are following suit and building cyber-warfare capabilities.

Der Spiegel terms the development of these aggressive hacking tools as Digital Weapons. In their view D weapons which should join the ABC (Atomic, Biological and Chemical) weapons of the 20th century because of their indiscriminate nature.

Here lies a fundamental problem. The modern world with connected global communications networks means that non-state actors such as civilians and businesses are now affected by the agencies' activities much more frequently than before. The internet is used by everyone – cyberspace is mainly a civilian space – and the opportunity for collateral damage is huge.

The papers leaked to Der Spiegel appear to show that signal agencies have little regard for the security and wellbeing of anyone who gets caught in the path of their operations. According to the documents, the agencies generally use the equipment of third parties – including innocent internet users - as an intermediate step for exfiltrating information form their operations. They even call them "unwitting data mules", and while in some cases they could be employees of companies, in other cases they appear to be quite random. This way the agencies cover their tracks and avoid being detected. But of course the unwitting victim could end up suspected of wrongdoing.

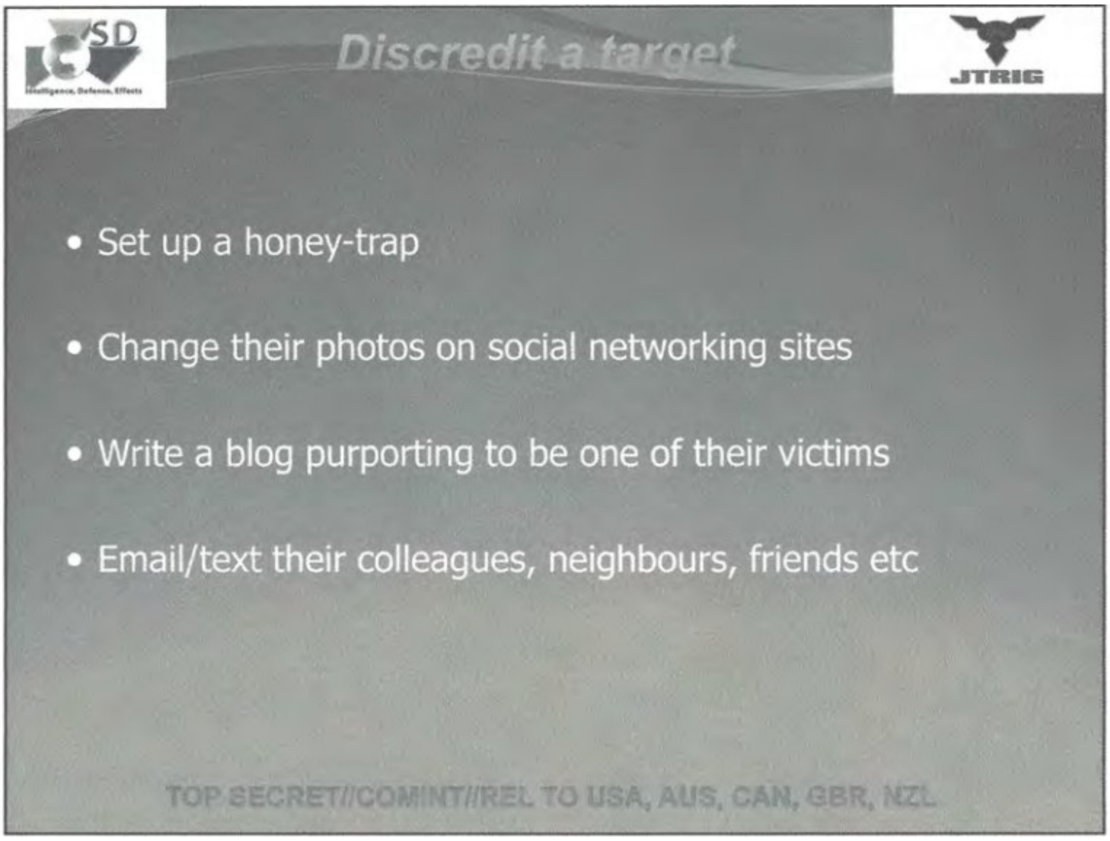
These is a thin line between many GCHQ activities and what is understood as "cyber warfare". The Tallinn Manual on the international law applicable to cyber warfare sets out that cyber attacks on civilians are unlawful.[iv] The agencies, oversight bodies and Parliament need to acknowledge that GCHQ has the capability to launch cyber attacks and confirm that procedures are in place to ensure that international laws of war are followed. These aspect should be part of the public debates on mass surveillance and making the agencies fit for purpose in post-Cold War democracies.

Below we outline some of the most controversial documented practices involving the UK.

5.2 Psychological operations against political activists

According to the Snowden documents, proactive actions,[v] now represent 5% of GCHQ's "business".[vi] Some of these actions will involve the hacking and disabling of target systems described in the previous sections. But GCHQ also appears to engage in dirty tricks and psychological manipulation programmes.[vii] The unit leading these efforts is called the Joint Intelligence Threat Research Group (JTRIG) with 150 staff trained in online covert operations, which they see as a third pillar of activities complementary to signals intelligence and computer network exploitation[viii].

Some of these operations[ix] are designed to intimidate and "pull groups apart"[x], for example, deleting a target's online presence and spreading false information. Leaked documents show that GCHQ has developed a programme to influence the outcome of online polls.[xi]


SD
Intelligence, Defence, Effects
JTRIG

Discredit a target

- Set up a honey-trap
- Change their photos on social networking sites
- Write a blog purporting to be one of their victims
- Email/text their colleagues, neighbours, friends etc

TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

GCHQ has used these techniques against groups not involved in terrorism or serious crime, such as the "hacktivists" of Anonymous.[xii] GCHQ has also targeted supporters of Wikileaks,[xiii] albeit in a less aggressive manner.

Any law breaking activities by political activist networks that may be disruptive but that are at their core non-violent social movements – from sufragettes to anti-fracking - should be dealt with by the criminal justice system, not a secretive spy agency. Any members of lawful organisations or groups not primarily engaged in criminal activity should not have their privacy or freedom of expression disproportionately interfered with.

5.3 Using illegal attack techniques: denial of service

Besides engaging in psychological warfare and the mass implants of malware, GCHQ has engaged in disabling remote systems through Denial of Service (DOS) attacks. This involves flooding the capacity of a networked computer system until it collapses.

According to documents published by NBC[xiv], Anonymous's chat rooms were shut down by GCHQ's own hacking operations in 2011, called Rolling Thunder, with the effect of pushing away some 80% of visitors.

According to NBC, this is the first time that a Western government has been found carrying that sort of attack, normally attributed to Chinese and Russian covert operations. The report also pointed out the impact on other websites and servers in the vicinity:

"a DDOS attack against the servers hosting Anonymous chat rooms would also have shut down any other websites hosted by the same servers, and any other servers operated by the same Internet Service Provider (ISP), whether or not they had any connection to Anonymous. It is not known whether any of the servers attacked also hosted other websites, or whether other servers were operated by the same ISPs"[xv].

Denial of Services are criminal acts and in the UK,[xvi] and a major reason GCHQ was persecuting many of those "hacktivists" was their use of this technique to shut down websites.[xvii] It now appears that GCHQ was using the same techniques against them. These attacks can have negative effects on computer systems in the vicinity, so innocent websites could be taken down as well, depriving many people of their freedom of expression.[xviii] A basic tenet of democracy is that security services must uphold the law when fighting those who break it.

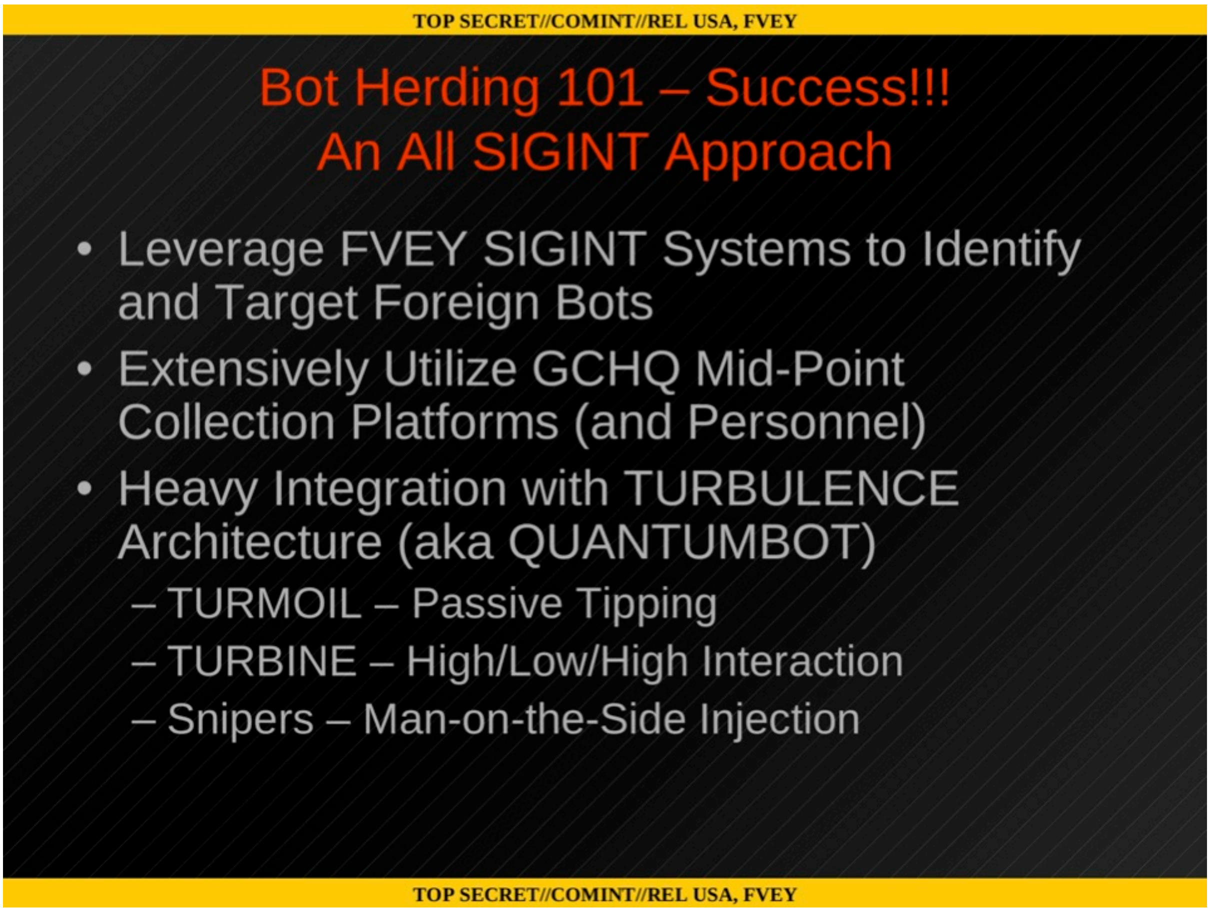
5.4 Fourth party collection

The NSA routinely piggy back on cyber offensive operations of other nations to steal data. Documents give an example where North Korean equipment had been bugged by South Korea, but the NSA managed to extract the information.[xix] Internal documents from Menwith Hill station in the UK describe how they use Kurdish intelligence activities to obtain information in Iraq and Iran[xx].

There should be clear regulations to ensure these operations do not give innocent civilians or businesses unwarranted exposure to risks.

5.5 Take over networks of hijacked computers

Leaked documents show the NSA has programmes dedicated to the acquisition of command and control capabilities over large networks of computers.[xxi] These so-called botnets, have been previously hijacked by criminals or other organisations. The operations under the programme DEFIANTWARRIOR rely on extensive support from GCHQ and use all the TURMOIL, TURBINE and XKEYSCORE technologies described above to discover and hack into the systems.



TOP SECRET//COMINT//REL USA, FVEY

Bot Herding 101 – Success!!!
An All SIGINT Approach

- Leverage FVEY SIGINT Systems to Identify and Target Foreign Bots
- Extensively Utilize GCHQ Mid-Point Collection Platforms (and Personnel)
- Heavy Integration with TURBULENCE Architecture (aka QUANTUMBOT)
  - TURMOIL – Passive Tipping
  - TURBINE – High/Low/High Interaction
  - Snipers – Man-on-the-Side Injection

TOP SECRET//COMINT//REL USA, FVEY

The controlled computers can then be used for further internet monitoring or “throw-away non-attributable” nodes for hacking operations. The leaked slides warn operatives not to show too much skill to avoid being identified as “state actors”.

The owners of infected computers will not notice that their computers are now involved in NSA/GCHQ operations. The NSA seems to limit takeovers to foreign botnets, which may provide some legal cover. But it is unclear what is the exact legal justification for the involvement of GCHQ.

5.6 Conclusion

Cyberwarfare and offensive capabilities are highly problematic. As we have seen in other chapters, these capabilities have a natural tendency to grow from possession of key points in the infrastructure (Chapter 1) and creation of capabilities to control other people's equipment and networks (Chapter 2). This is aided by the intense integration of capabilities and technology between the USA and UK.

Once GCHQ has control of both the network and specific networks in foreign countries, the possibility of using the control of networks to attack systems in other countries becomes obvious. The same tool can be used to surveil or shut down.

The problem however with GCHQ controlling these offensive capabilities is that they are highly secretive and are not subject to the same levels of public oversight we would normally expect. Parliament would normally examine the ethical, legal and strategic questions associated with our offensive weaponry.

Cyberwarfare capabilities of course have profound implications. The uses they can be put to are potentially horrific, and likely to implicate the general population. Since nearly all modern systems are computerised, nearly anything connected to the Internet can potentially be weaponised. So cyberware could be used against infrastructure that is controlled by specific civilian or military equipment – for example, an electricity grid, nuclear power plant or transportation controls.

There are open questions surrounding the need for specific international law to govern cyberwarfare. While our government believes there is no need for new treaties, it is Parliament's job to consider whether it currently understands the capabilities we are developing in secret and whether our clandestine approach supports or undermines that view.

Finally, we should clearly limit the scope of what is understood as cyberwarfare. The framing of many issues around digital security in these terms has been criticised by scholars such as Myriam Cavelty[xxii]. She argues that the excessive use of war-like language to talk about complex phenomena - where traditional enemy lines are unclear - can hinder a proper analysis and trigger disproportionate responses.

[i] http://www.spiegel.de/international/world/new-snowden-docs-indicate-scope-of-nsa-preparations-for-cyber-battle-a-1013409.html

[ii] http://www.washingtonpost.com/world/national-security/us-spy-agencies-mounted-231-offensive-cyber-operations-in-2011-documents-show/2013/08/30/d090a6ae-119e-11e3-b4cb-fd7ce041d814_story.html

[iii] https://www.gov.uk/government/news/strategic-defence-and-security-review--3

[iv] Schmitt, M. N. (2013). *Tallinn manual on the international law applicable to cyber warfare* (pp. 1–215). New York: CAMBRIDGE UNIVERSITY PRESS.

[v] https://firstlook.org/theintercept/document/2014/04/04/full-spectrum-cyber-effects/

[vi] http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive2_nbc_document.pdf

[vii] http://msnbcmedia.msn.com/i/msnbc/Sections/NEWS/snowden_youtube_nbc_document.pdf

[viii] https://www.eff.org/files/2014/04/09/20140224-intercept-training_for_covert_online_operations.pdf

[ix] http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_cyber_offensive1_nbc_document.pdf

[x] https://www.eff.org/files/2014/04/09/20140224-intercept-training_for_covert_online_operations.pdf

[xi] https://firstlook.org/theintercept/2014/07/14/manipulating-online-polls-ways-british-spies-seek-control-Internet/

[xii] http://msnbcmedia.msn.com/i/msnbc/sections/news/snowden_anonymous_nbc_document.pdf

[xiii] https://firstlook.org/theintercept/article/2014/02/18/snowden-docs-reveal-covert-surveillance-and-pressure-tactics-aimed-at-wikileaks-and-its-supporters/

[xiv] http://www.nbcnews.com/feature/edward-snowden-interview/war-anonymous-british-spies-attacked-hackers-snowden-docs-show-n21361

[xv] http://www.nbcnews.com/feature/edward-snowden-interview/exclusive-snowden-docs-show-uk-spies-attacked-anonymous-hackers-n21361

[xvi] http://www.out-law.com/page-9592

[xvii] http://www.techdirt.com/articles/20140205/09440926098/those-convicted-ddos-attacks-uk-wondering-why-gchq-was-allowed-to-ddos-them.shtml

[xviii] http://www.infosecurity-magazine.com/view/36789/gchq-used-ddos-attack-on-anonymous-communications/

[xix] http://www.spiegel.de/media/media-35679.pdf

[xx] http://www.spiegel.de/media/media-35680.pdf

[xxi] http://www.spiegel.de/media/media-35689.pdf

[xxii] https://ccdcoe.org/publications/2012proceedings/2_6_Dunn%20Cavelty_TheMilitarisationOfCyberspace.pdf