Chapter 2

2 Invasive collection: active signals development

2.1 Introduction

In the previous section, we looked at how we all generate data by using the Internet, phones, apps and even wearable technology, and how the NSA and GCHQ collect anything that passes through wires or the ether. But the agencies gather even more information through a range of intrusive techniques to extract data from machines that the agencies call Active Signals Intelligence.

Interference with equipment is not new. GCHQ has always carried out clandestine operations. During the 1950s and 60s it was routine to try to plant listening devices in foreign embassies and other targets as part of the Cold War.[i] UK legislation allows agencies to obtain authorisation to carry out this kind of "equipment interference".

Most people will broadly understand operations targeting clear military, diplomatic or security objectives; for example, hacking into a terrorist phone, possibly even the tapping of a cable feeding the part of the city where a foreign embassy is located. But the Snowden documents show that in recent times these activities have evolved into something else.

For a start, the capability to carry out some such attacks in the digital age will rely on softening the infrastructure of the Internet, by weakening widely used security systems, which can have consequences for all of our online safety.

In addition, there is now evidence that the agencies develop hugely complex operations that target a very broad range of organisations and individuals, including innocent civilians, in order to get to their target.

Finally, the scale of the potential activities has grown excessively. The NSA and GCHQ are able to target millions of computers. Termed Computer Network Exploitation, the agencies are building a global machine capable of hacking on an industrial scale.

In the previous section we saw how passive state surveillance has become massive and nowadays affects not just terrorists, diplomats and high tech companies, but everyone who uses modern communications. Here we explain how the active and more invasive aspects have also expanded to potentially affect every one of us. It is hard to imagine that the programmes are under effective control.

2.2 Documented examples of attacks

2.2.1 Belgacom and German satellite businesses

The Belgian telecommunications company, Belgacom, was targeted by GCHQ from 2010 in order to gain access to important international telecommunications infrastructure.[ii] This is the first documented government-sponsored cyberattack of one EU member state on another.[iii]

Belgacom operates an important mobile phone roaming exchange that enables travellers to use their handsets in other countries. This was the main objective of the attack, but GCHQ also planned to access the company's international cables. Thanks to this attack, GCHQ had potential access to the communications of all European institutions based in Brussels, although there is no documented evidence that these were targeted in this way[iv].

Operation Socialist, as GCHQ codenamed it, began by creating fake LinkedIn webpages in order to infect the computers of individual Belgacom engineers with malicious software. The software infections eventually reached the core of the company's internal network, and even now it is unclear whether their systems have been completely cleaned.

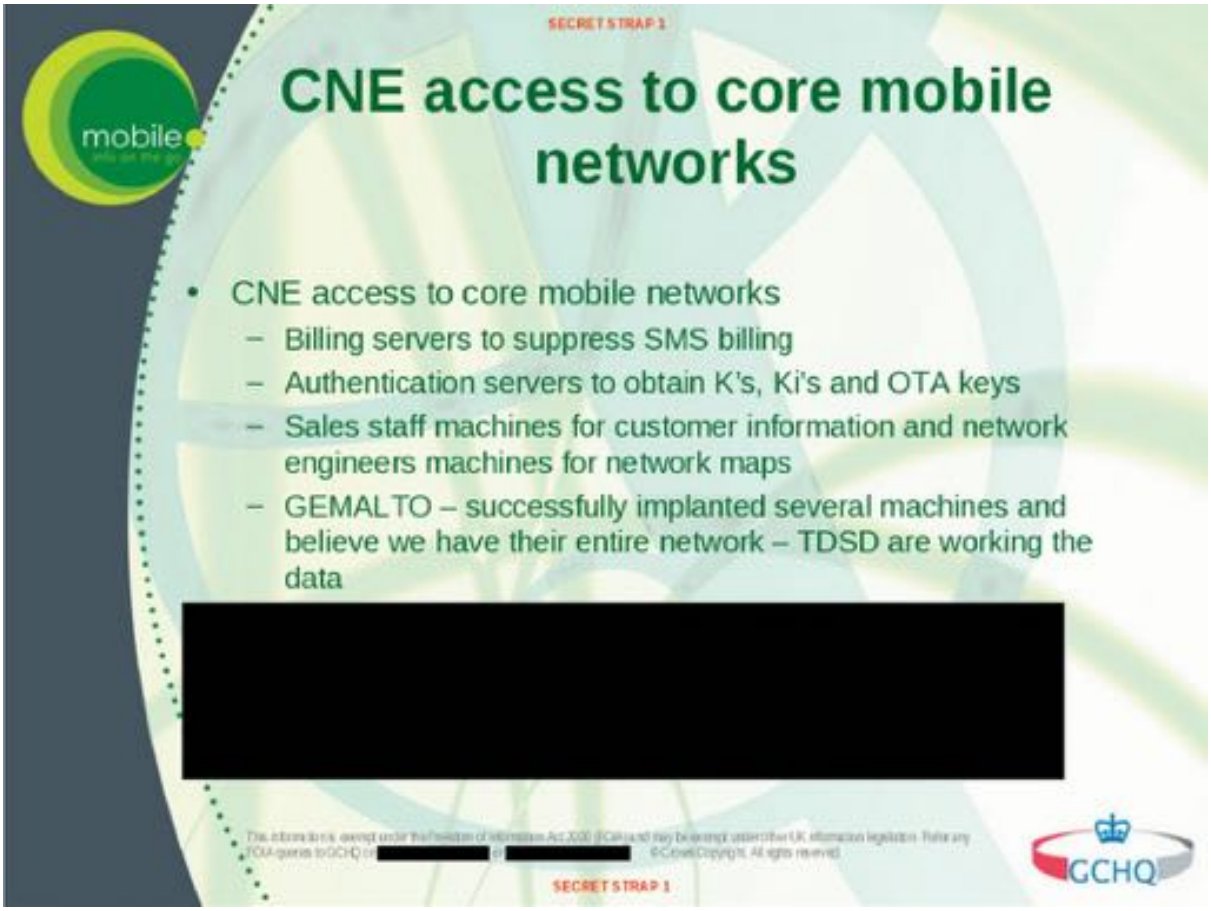
The malicious software (malware) used in the attack has been identified as a very sophisticated programme called Regin, also found on European Union computers targeted by the NSA.[v] The software has been compared to the infamous Stuxnet virus, used against the

Iranian nuclear programme, which was called by Wired magazine “the world's first digital weapon”[vi].

There is currently a criminal investigation in Belgium into the attack, but both the Belgian Government and the company itself seem keen to hush up such an embarrassing diplomatic incident.

2.2.2 Gemalto SIM Card

In another well documented case, GCHQ attacked the Dutch company Gemalto, a major manufacturer of SIM cards used in mobile phones worldwide. The aim of the hacking operation was to steal encryption keys for mobile phones.[vii]



Encryption keys are only needed to intercept mobile traffic between the handset and the station, as that is the only moment when it is encrypted. Once the conversation enters the main telephony system it travels without encryption and could be harvested through one of many corporate partnerships. This indicates that the objective was targeted interception.[viii]

The documents also state that the agencies targeted other SIM card providers, and were unsuccessful that the time. But it is not know whether those were infiltrated at a later date.

2.2.3 Telecommunications companies

GCHQ has also attacked German providers of satellite data services: IABG, Cetex and Stellar.[ix] The joint NSA-GCHQ operation targeted exchange points linking satellites with the broader Internet, and identified 'important' customers of the German providers.

According to leaked documents, in 2013 the NSA had obtained legal authorisation under the FISA court system to monitor "Germany". It is unclear what the legal basis is for the British participation in the attacks.

The NSA and GCHQ also infiltrated several global telecom companies including German providers in order to gain access to the data flowing over their networks.[x] The aim was to produce intelligence on the architecture of the Internet in order to prepare other interventions. The attacks involved targeting individual employees of the companies.

2.2.4 TOR

GCHQ has a programme called EGOTISTICAL GIRAFFE that targets the TOR anonymous communications network.[xi] TOR "The Onion Router" is instrumental in enabling hundreds of thousands of political dissidents to access the Internet anonymously, and thus communicate without fear of repercussions in places like Iran and China. It is also increasingly used by regular Internet users in Western countries wishing to avoid snooping by commercial Internet companies. The development of TOR has been substantially financed by the US government.[xii]

TOR has recently come to prominence because its capacity to provide security and anonymity has also been used by criminals, including child abusers, and has enabled an underground market in illicit goods such as drugs. The current debates about TOR are reminiscent of the early days of the Internet, when it was perceived as an unregulated "electronic frontier". Most advocates of freedom of information agree that on balance TOR is a force for good, despite the potential for abuse by unscrupulous criminals – much like the Internet as a whole.

According to the NSA's own documents[xiii] GCHQ and NSA staff expressed their dislike for this tool in a presentation slide set called "TOR Stinks".[xiv] Despite their best efforts the agencies acknowledged they have not been able to fully crack the TOR network to de-anonymise the users.

Leaked source code from the XKEYSCORE system[xv] shows that operatives use it to systematically track TOR activity and potential users.

2.3 From equipment interference to industrial scale hacking

The NSA and GCHQ run a very complex global infrastructure that allows them to hack into millions of computers worldwide. This, in their own terms, "industrial scale exploitation"[xvi] allows the agencies to obtain information from these machines. However they are also able to remotely control the computers, including those of innocent people that are used as accessories to other covert operations. Many attacks target infrastructure such as routers.[xvii] In their documents, the agencies call these activities Computer Network Exploitation, and the term is also used in a recent public consultation by the Home Office on equipment interference[xviii].

Traditional interception attacks on individuals required either direct physical access to plant bugs, or targeted techniques that required considerable effort. But recently the US, the UK,

and other Five Eyes countries, have developed the capacity to automate remote hacking attacks, allowing mass computer infection on an industrial scale. The UK is heavily involved in the development and implementation of these mass hacking systems.

Leaked US budgetary details show that the use of such techniques has exploded in the last decade. In 2004 the NSA had some 100 to 150 active "implants".[xix] By 2014 the US had infected tens of thousands of machines with malicious software,[xx] with up to 100,000 computers being controlled at any time in order to act as platforms for hacking attacks[xxi] on third parties. We do not know how many computers are directly infected and controlled by GCHQ.

It is generally accepted that spy agencies must have some properly regulated targeted hacking capabilities, but it is concerning that the NSA and GCHQ are building systems capable of targeting millions of people. The legal basis for this is very unclear.

The top level components of this system have been extensively described in leaked documents. These programmes for mass hacking[xxii] involve many interconnected subsystems.

The following is a very superficial description based on the available information[xxiii] and analyses put together by security experts. The source leaked documents are highly technical and it may be challenging to fully understand the operations. Given that new revelations continue to appear it is likely that this information will become quickly outdated.

The scale of operations is staggering, and in many cases there is a blurring between mass surveillance and hacking, with access being used to plant malware in network infrastructure that is then used to enable new channels for bulk collection.

2.3.1 The NSA hacking budget: GENIE

The NSA GENIE programme appears to be a massive umbrella for a very broad range of activities and programmes[xxiv] for the exploitation of equipment. The NSA allocated more than 650 million dollars in 2013 alone, with the projected budget passing the billion dollars mark in 2017.

Many but not all of the programmes described in this section are part of GENIE.

The documents about GENIE contain information marked for sharing with the Five Eyes countries, and is evidence of a very close working relationship between these partners.

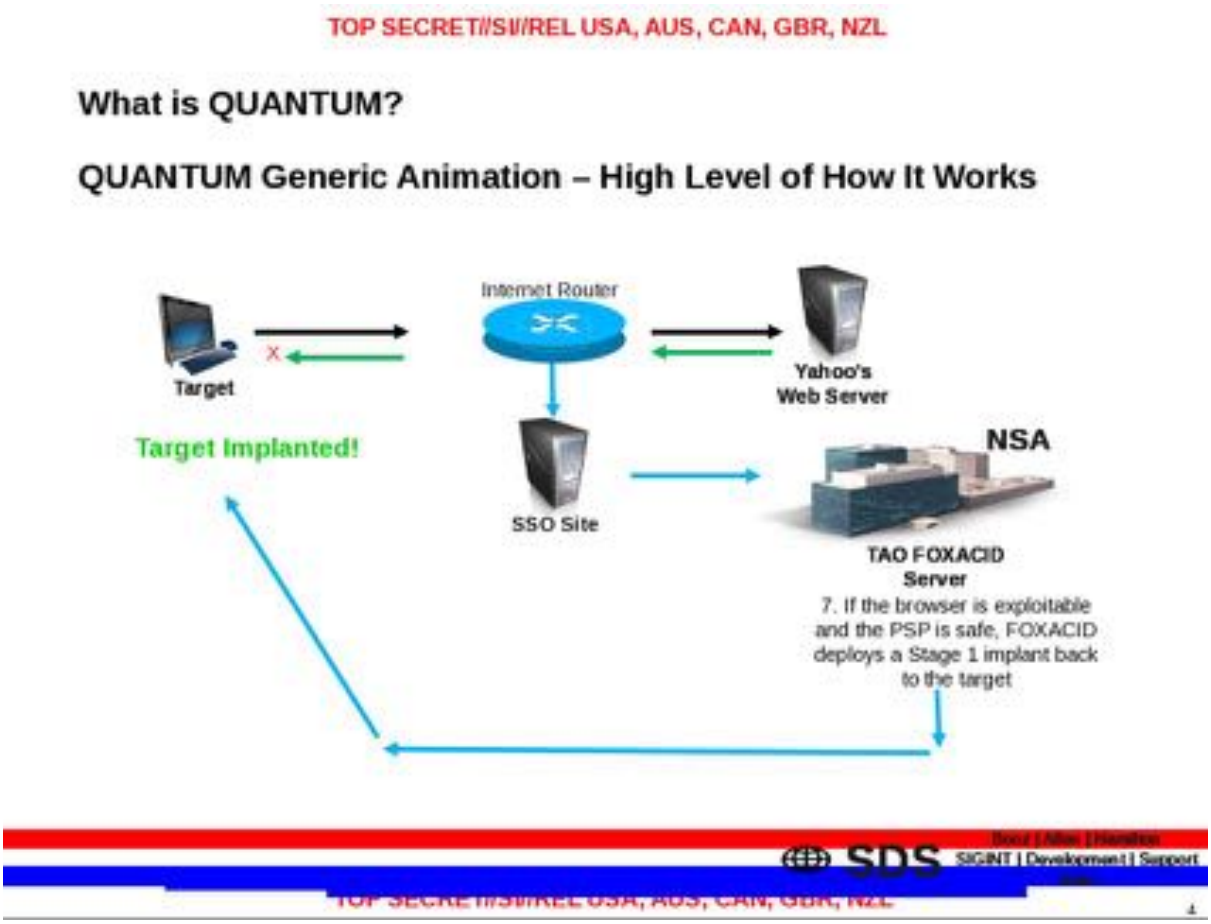
2.3.2 Reaching the target: QUANTUM

QUANTUM like many of these security codenames, describes a complex system with several components. The system enables an operative to task the hacking of specific computers, but also has the ability to interfere with Internet traffic in real time in order to infect target equipment. Another component provides the ability to introduce malware into a very broad range of equipment. The agencies have developed many tools (see slide below) specialised in

impersonating particular types of websites or computer equipment. By fooling the target's computer or mobile phone into believing it is communicating with a genuine source they can trick them into accepting malicious software.

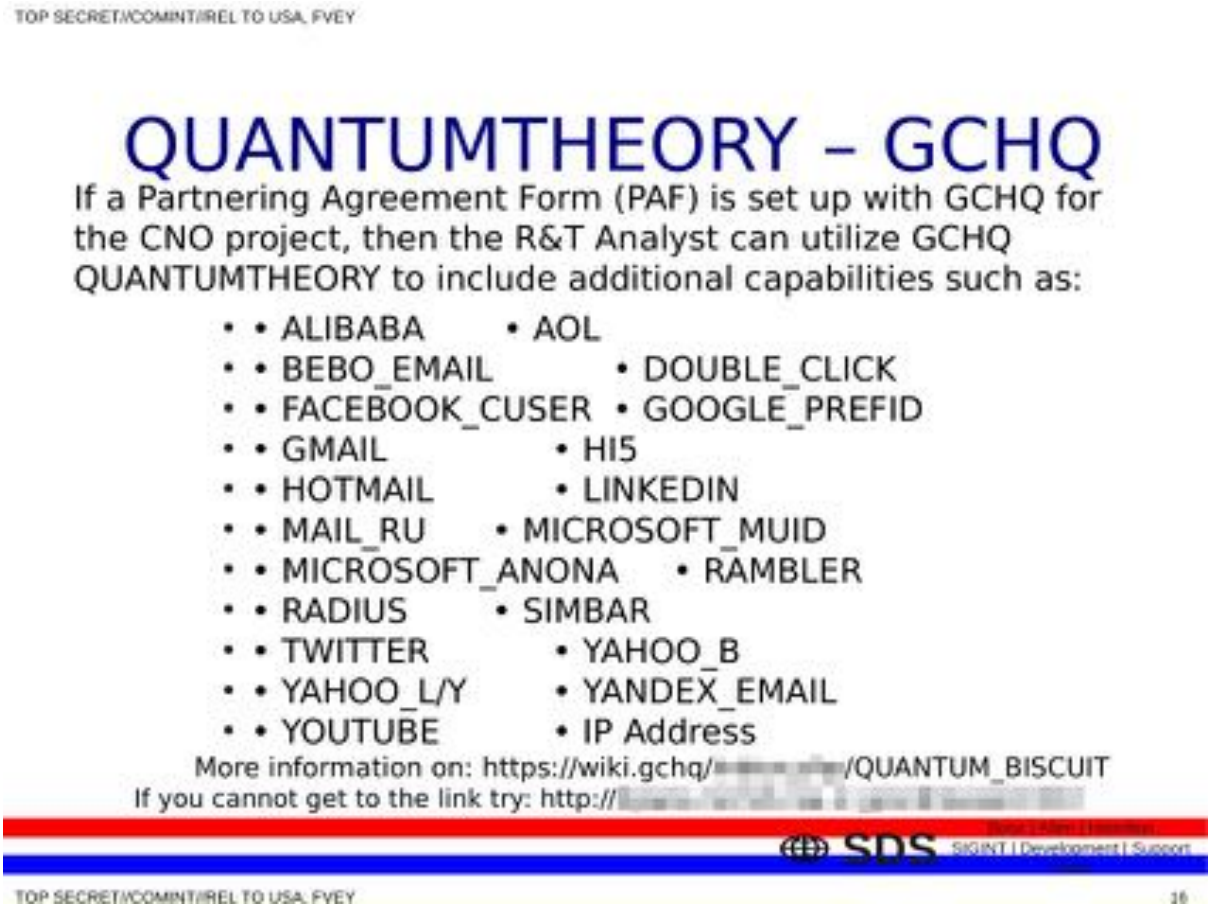
The process starts with a senior analyst sending a request for an operative to hack the equipment of a target. This involves providing emails or other data associated with the target, achieved through various means, including database searches and other monitoring tools.

Once identified and authorised, the target's information is sent to the global network of machines at key choke points of the global Internet infrastructure involved in bulk collection. These computers will keep an eye for the target to appear, and when activity is detected this will trigger a so-called "man on the side attack". There is evidence that these implants are also aided by the hacking of Internet infrastructure such as routers.[xxv]



The attacks are mainly based on making the target's equipment believe it is communicating with a genuine source of information through the technical impersonation of software and hardware. Unsuspecting targets browsing Facebook or LinkedIn will not realise that the NSA has added some code to those websites that will infect his or her computer. This was the way that engineers working for Belgacom were infected by GCHQ.

There are many documented types of QUANTUM tools[xxvi]. These are not the actual software that will spy on the target or disable the equipment, but the tools that enable its delivery. These include tools for impersonating any computer, hijacking online messenger sessions, and even controlling networks of zombie computers, called botnets.



Menwith Hill in the UK is named in documents as one of the bases where QUANTUM[xxvii] is used to target Yahoo and Hotmail. There is evidence of GCHQ's involvement in QUANTUM, and the expansion of the programme to include other allies, such as Sweden[xxviii].

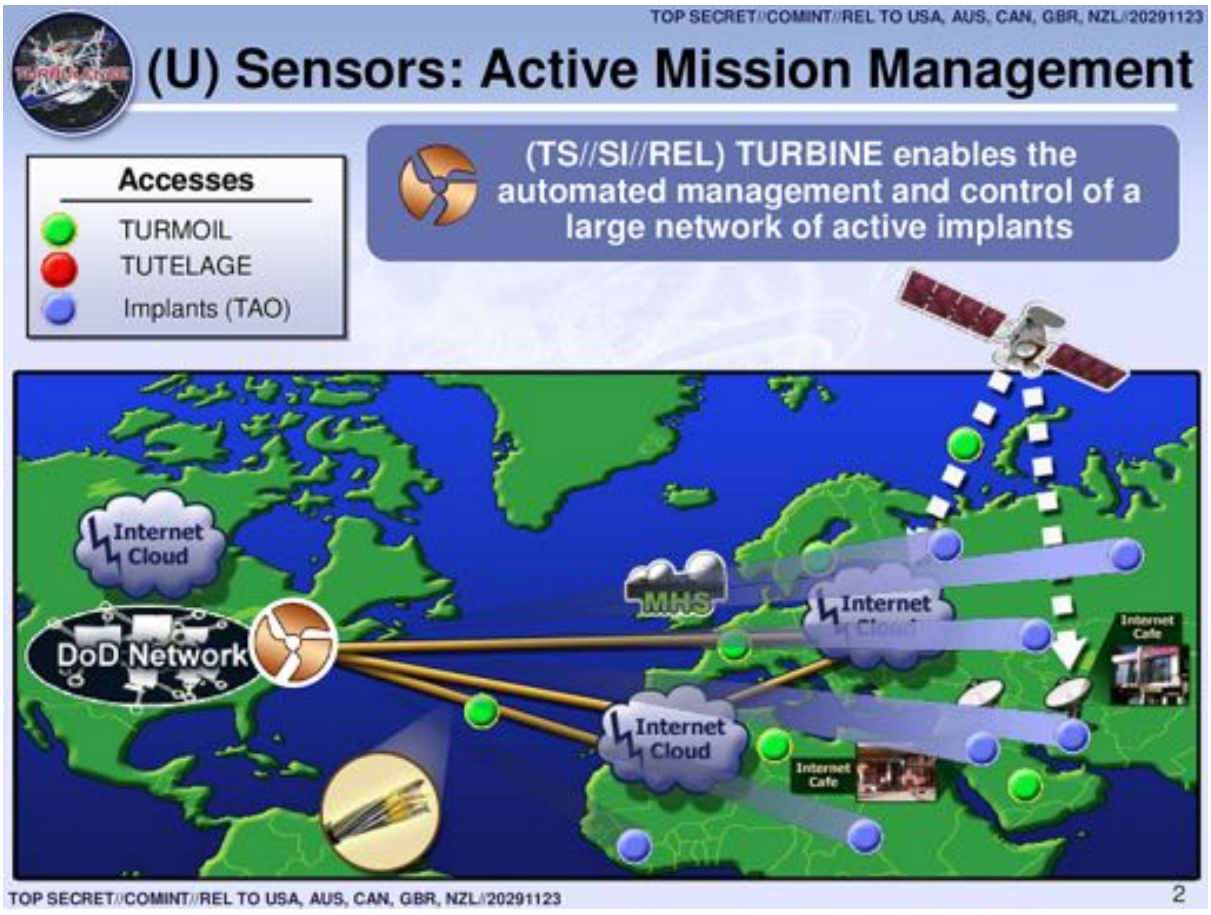
2.3.3 Automated tailoring and delivery of malware: TURBINE

TURBINE is an artificial intelligence system that automates remote hacking by tailoring the attacks to that particular target's computer or phone and their activities. For example, if a

person of interest is trying to access Facebook using Firefox version 12 in a Macbook model 2010, TURBINE will find the appropriate software tools.

The system will also automate the retrieval and collection of information from the infected computers.

The predecessor programmes to TURBINE under GENIE were able to control some 85,000 implants in strategically chosen machines around the world in 2011. With over 1,000 dedicated staff the NSA was able to only use some 6,000 of those.[xxix] By removing human intervention, the new "command and control" tool allows for a huge scaling up of this kind of operations, which is describe in documents as one of the greatest challenges in this area of activity.

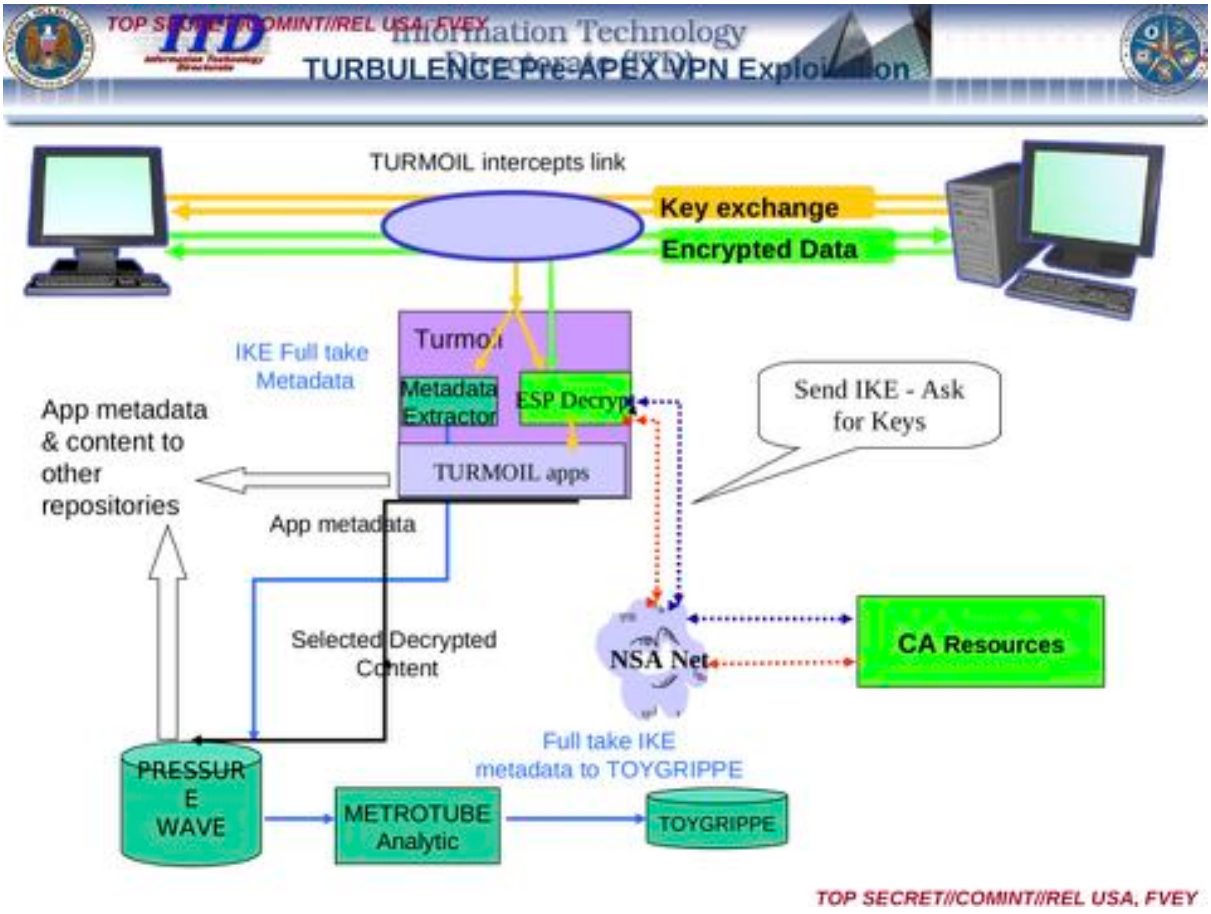


Once a target has been confirmed and TURBINE has chosen one of the many tools in the NSA/GCHQ arsenal of spying software, the latter is sent back to the target. In order to do this the agencies use another set of tools called QUANTUM.[xxx]

2.3.4 Access to the high speed backbone: TURMOIL and TURBULENCE

The TURMOIL network we mentioned in the section on collection is composed of the points of direct access to the global communications system, such as cables and satellites, on cable interception. This is a critical component of the UK/US global surveillance complex. As we saw, the components of TURMOIL are involved in bulk collection and processing of data, many being part of the XKEYSCORE system. But in addition they allow the agencies not only to monitor Internet traffic for specific targets, but to perform targeted attacks against them.

TURMOIL is connected with a huge apparatus dedicated to breaking encryption as part of the NSA programme[xxxi] TURBULENCE. This includes being able to connect to tools that allow them to bypass encryption in types of traffic such as Virtual Private Networks.



TURMOIL also provides support for the injection of malware as part of the QUANTUM process. The direct access to the Internet backbone is central for everything the agencies do: collection, interference, decryption and so on.

TURBULENCE is also used by the US as a defence against foreign cyberattacks[xxxii]. It is possible that similar activities take place in the UK.

2.3.5 An endless arsenal of digital weapons

The state of the art system appears to be based on the interdependence of all those systems: TURMOIL detects, TURBINE decides and QUANTUM attacks, delivering the malware.

Leaked documents show that the NSA and GCHQ have an extensive arsenal of malware and other hacking tools to convert any computer or mobile phone into a spying machine.[xxxiii]

Security researcher Claudio Guarnieri[xxxiv] gives an excellent overview of the main technologies and programmes available to the NSA and GCHQ.

The agencies initially use a tool to gather basic information about the device and prepare for further infection, called VALIDATOR. It comes in many varieties and uses sophisticated techniques to get the data out of the infected machine undiscovered.

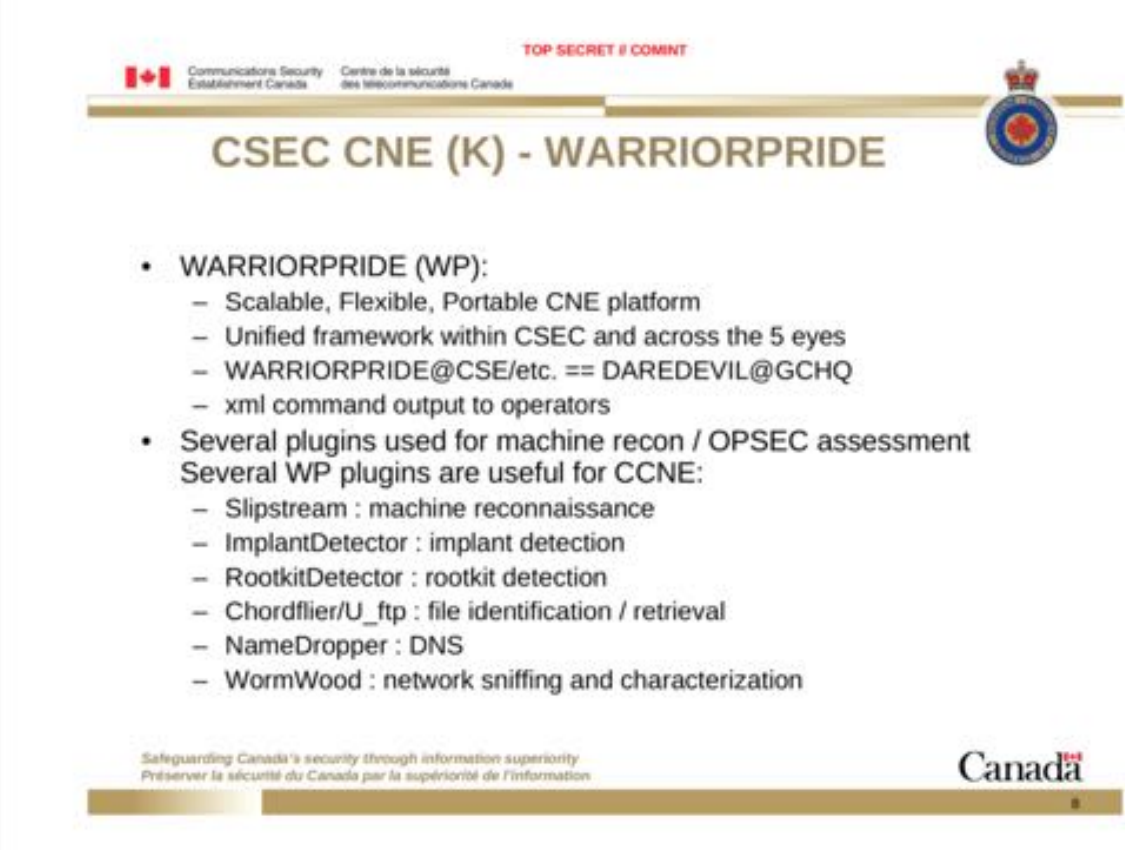
The agencies also have a system of modular plugins for accessing different parts of a machine under the programme UNITEDRAKE. These include the following:

GUMFISH takes over webcams to record images.

- CAPTIVATEDAUDIENCE turns on the microphone to record audio.
- FOGGYBOTTOM collect all Internet activities, including passwords for websites and email accounts
- GROK will log all keystrokes entered into a device

In addition, a similar but more sophisticated programme called STRAITBIZARRE allows for infected machines to be used to direct further attacks on third parties via QUANTUM.

WARRIORPRIDE is a similar system developed in a joint effort by the Five Eyes.[xxxv] This project may appear in British documents under the term DAREDEVIL. GCHQ's slides show that the system has been used to target iPhones with the development of a specific QUANTUM vector tailored to the Safari browser.[xxxvi] The tool allowed the extraction of contacts, messages, call logs, notes, location history and photos.



GCHQ developed a series of plugins to extract information from mobile devices, targeting both Android and iPhones. Under names such as NOSEY SMURF these tools can retrieve almost any content from a phone.[xxxvii]

Researchers from security firm Kaspersky have found evidence that the Regin malware involved in the hacking of Belgacom and EU computers is also probably part of this project[xxxviii].

2.4 Breaking Internet security

Most of the information transmitted on the Internet is transparent - many websites will want to be as accessible as possible - and can be read by whoever can intercept it. But an increasing amount of the information circulating on the Internet – and collected by GCHQ – will not be immediately accessible to everyone because it has been made unreadable through encryption.

This technology used to be used exclusively by governments and large companies, but it is now widespread, forming the basis for many online commercial activities, such as banking

and shopping. It is becoming increasingly common in other private communications, e.g. social networks and email traffic, whenever some level of confidentiality is sought. For example, without encryption search terms inputted into Google are sent transparently online, including any embarrassing items such as Sexually Transmitted Diseases. Without encryption, emails are just like postcards. Encryption allows the modern Internet to function.

The Snowden documents revealed that the NSA and GCHQ see encryption with great hostility, and have successfully managed to break through some of the key encryption technologies used to secure the Internet.[xxxix]

This is something that has caused major consternation among Internet experts and the technical community. The fundamental problem is that once a weaknesses is created in a security system there is no guarantee that it will only be used by Western agencies for legitimate purposes. Criminals and other agencies can discover and use the same techniques.

In response, over 50 of the world's foremost experts on computer security signed an open letter[xl] where they urged the US government:

"to reject society-wide surveillance and the subversion of security technology, to adopt state-of-the-art, privacy-preserving technology, and to ensure that new policies, guided by enunciated principles, support human rights, trustworthy commerce, and technical innovation."

Documents released by The Guardian[xli] newspaper and other media in 2013 brought to light the existence of the BULLRUN programme of the NSA to break privacy and security technologies. The documents show that the UK has access to BULLRUN, with plans to integrate the other Five Eyes partners.

GCHQ also has a similar programme called EDGEHILL dedicated to breaking specific Internet encryption systems. The leaked documents showed that its initial purpose was to decode encrypted traffic from three main Internet companies and thirty types of Virtual Private Network (VPN). GCHQ was also working to break the encryption of the main providers of email and private messaging – named in the document as Hotmail, Google, Yahoo and Facebook. But it has predominantly focused on Google "due to new access opportunities being developed." In 2015 GCHQ hopes to have cracked the codes used by 15 major Internet companies and 300 VPNs.

A large amount of leaked documents on these activities by the NSA and GCHQ were published by the German magazine Der Spiegel in December 2014.[xlii] These provide a much richer picture of the state of the agencies war on Internet security.

The released documents show among many other things that the agencies:

Are able to access encrypted Skype conversations.

- Planned to be able to break into 20,000 VPN communications per hour by the end of 2011.
- Consider recording private Facebook chats a minor task.
- Find that different email providers present various levels of difficulty depending on the level of encryption they use.
- Routinely break through the SSL used to securely access websites, with the NSA aiming to crack 10 million intercepted https connections a day by late 2012.

The agencies appear to have problems with a number of technologies:

Truecrypt file encryption

- OTR chats
- TOR anonymous browsing
- ZRTP video and audio conferencing
- Open source projects generally tend to be more robust

According to the leaked documents, the agencies overcome encryption through a combination of approaches. The main documented avenues for the agencies to break Internet security are:

- Weakening standards, policies and specifications.

- Building backdoors through corporate partnerships.
- Exploiting existing vulnerabilities instead of reporting them.
- Actively attacking technologies.

Weakening the security of cryptographic systems has been commonplace in the world of spying agencies. In a well-documented case, GCHQ and the NSA subverted the operations of Swiss company Crypto AG, a provider of strong crypto tools that could be bought by third party countries. But those operations remained within the realm of the shadowy world of spies. The current activities of the agencies affect anyone and everyone as we all rely on secure computer systems to run and participate in our societies and economies.

2.4.1 Weakening standards

Many attacks are successful because the agencies have previously worked to weaken the underlying technologies and standards. In some cases this takes place before they are implemented, during the design and development stage, for example through the infiltration of projects to create backdoors.

The existence of such weaknesses has been accepted for some time, but it is generally very hard to prove they were intentionally created. However, released documents confirm "the fact that NSA/CSS makes cryptographic modifications to commercial or indigenous cryptographic information security devices or systems in order to make them exploitable".[xliii]

Leaked documents from GCHQ[xliv] show that NSA agents were involved in discussions at the Internet Engineering Task Force (IETF), the technical body in charge of ensuring the functioning of the Internet. In one case, the agents discussed the opportunities presented by new technical developments in Voice over IP (VOIP) to improve their ability to target communications.

2.4.2 Corporate partnerships

Although there is no available data for the UK, the NSA spent some $250 million a year working with Internet companies to insert back doors into encryption products.[xlv] At the very least it seems extremely likely that GCHQ directly benefits from these activities. We can only speculate that the agencies expect that nobody else will notice that those holes exist, but there is no way to assure that will be the case.

These practices have long been documented. Microsoft, Lotus and Netscape all provided a backdoor for the NSA to access the encrypted communications of non-US customers.[xlvi]

In a particularly troubling case, US security company RSA denies accusations that it was paid $10M by the NSA for introducing some recently discovered flaws in their products used by thousands of companies and governments worldwide. The company argued that they collaborated with the NSA in good faith, trusting them to provide secure technologies.[xlvii] Whatever the truth, it is clear that security companies that up until now have collaborated with the agencies with integrity will be less trusting of the NSA and GCHQ in the future.

The agencies also try to obtain the open collaboration of technology companies without subterfuge. There are reports that the NSA has directly asked for the master keys that would allow them to decrypt all the email from Gmail and Yahoo.[xlviii] Internet companies strenuously deny providing any such keys.

When they run out of other options, the agencies can attempt traditional infiltration. Leaked documents show that GCHQ has a human intelligence operations team (HUMINT) responsible for identifying, recruiting covert agents in the global telecoms industry.[xlix]

2.4.3 Exploiting vulnerabilities

The NSA and GCHQ appear to make use of existing vulnerabilities in software and hardware that create risks to the wider Internet community. The agencies use any available opportunity to gather data, without a proper framework for analysing the risks and wider societal costs of their acts and omissions.

Security problems are generally made public in a controlled process, called responsible disclosure. People who discover these problems tell the creators of the original product before making it public. This allows the manufacturer or developer to provide a fix at the same time that it warns customers of the issue. The delay until the fix is implemented by customers is often exploited by criminals and hackers. It is sometimes a matter of minutes for attacks to take place, as within the first 24 hours many vulnerable systems will have been fixed.

There is a thriving market in so-called "zero day exploits".[l] The zero refers to the number of days since the vulnerability was published, meaning they are not public. Unfortunately, instead of clamping down on this market, security agencies and military businesses are becoming the main customers.[li] In leaked documents these purchases are termed "community investment"[lii], with the NSA spending some $25 million in 2013 buying software vulnerabilities.

Bloomberg reported that the NSA had been exploiting the infamous Heartbleed[liii] bug for two years, instead of trying to fix it.[liv] If true this would mean that the agency has put its internal mission ahead of the security of millions of companies, banks and individuals.

Both US and UK agencies have a wider public responsibility to provide Internet security in addition to their spying activities. This involves collaborating with many companies,[lv] in some cases obtaining prior notification of vulnerabilities. This may sound reasonable from the perspective of public protection, but given what we know now it may be wise to review these roles.

2.4.4 Direct attacks

The documents leaked by Der Spiegel in 2014 provide evidence of the many complex techniques used by the NSA and allies to attack encryption. A detailed analysis is beyond the scope of this paper.

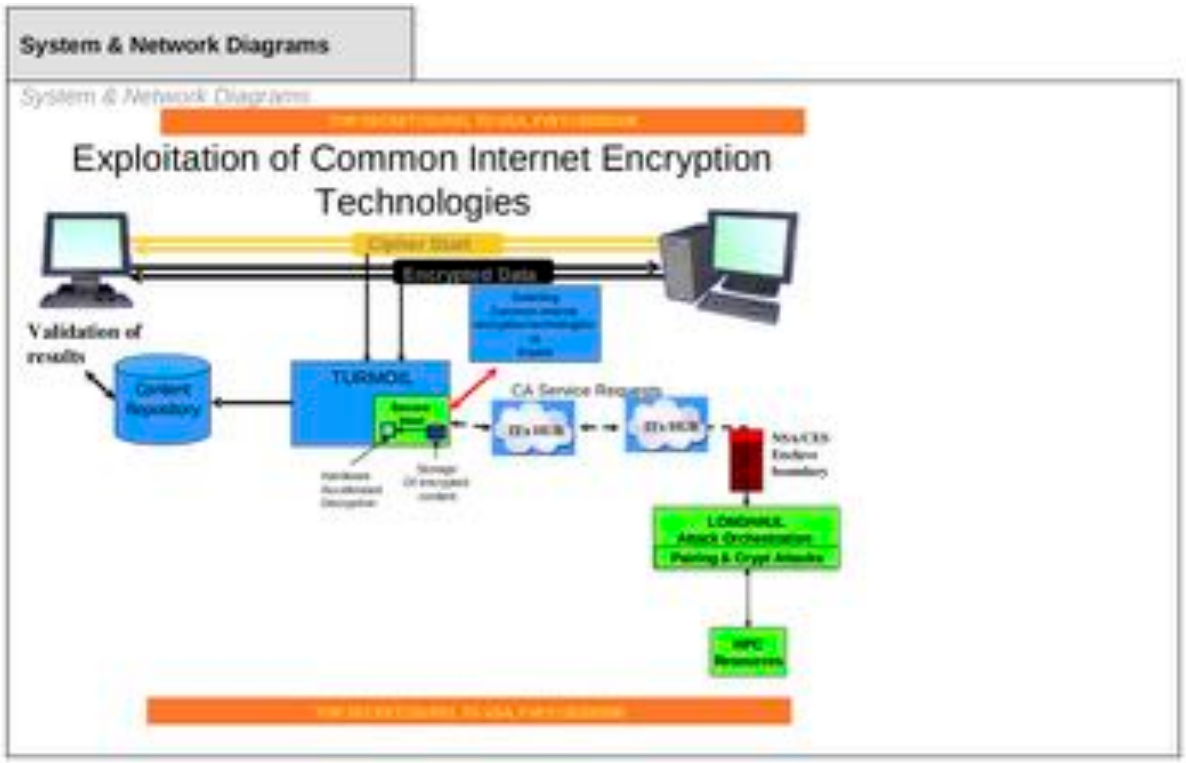
The documents provide a summary of BULLRUN's main activities:

Computer network exploitation (being able to intercept and modify traffic)

- Collaboration among agencies
- High performance computers
- Development of advanced mathematical techniques.

GCHQ collects billions of cryptographic exchanges between Internet users and the services they access, such as Google, Facebook or Yahoo.[lvi] The FLYING PIG database is used to build intelligence on these technologies to help target efforts. But it involves collecting the information of millions of Internet users. This project is associated with BULLRUN, showing that GCHQ is not just receiving US technology, but actively collaborating in its development.

GCHQ runs joint experiments with the NSA to try to break website encryption, including through the use of hardware accelerated decryption and use of resources from Certificates Authorities[lvii], which supposedly guarantee the authenticity of websites, among other techniques. The image below shows the architecture of one such experiments. It is unclear



whether it was successful.

It is important to understand the difference between the encryption itself, which is the mathematical scrambling of the information, and the protocols and tools used for the processing and exchange of encrypted information. It has been stressed by most sources and experts, including Snowden, that it is the latter that has been mainly affected. Strong pure mathematical cryptography remains viable in many cases and many encryption technologies remain out of the reach of the security services, as we saw above.

2.5 Conclusion

We see the same pattern of UK and US operational and technological integration. There aso is a sense of the UK doing USA's dirty work.

Invasive collection brings in new innocent bystanders – in this case companies or computers that become part of GCHQ botnets or compromised networks. This is the precise opposite of targeted interference and is hard to justify as well as being surprising. Can it be justified when foreign companies could be asked for their co-operation through the legal regimes of the countries concerned?

The underlying sense is that equipment interference should be taking place only when the legal regime cannot be used, but is actually being used when it is hard to ask for co-operation. This may be because international regimes may not permit it. This is different to being impossible because the target is an actual enemy or person of interest. This is a significant blurring of lines.

We have also seen how the mass surveillance infrastructure GCHQ possesses, in particular access to cables, is used for network injection techniques to enable equipment interference. This represents another huge form of leverage of our strategic position on the international Internet network with profound implications.

Industrial scale hacking also blurs the line between intelligence and the use of hacked equipment for offensive purposes. The same techniques can be used for different purposes; anything that is hacked can also be switched off or made to malfunction. Depending on what the equipment is controlling, it can therefore be weaponised. We return to this in Chapter Five, when we consider the offensive capabilities that GCHQ possesses.

Issues around Internet security are also very problematic and deserve thorough consideration. It is hard to justify and measure the problems that will be caused.

In general the evidence in the chapter shows the tension between the desirability for collective personal security versus the desire of national security to ensure a level of insecurity for everyone. In order to invade equipment, it has to be insecure. The fundamental aim of the agencies, our security, becomes a barrier to the way they operate.

Is it tenable to maintain a measure of collective insecurity to enable surveillance, when security is so central to everyone's online activities? This is a complicated question, and we turn to the consequences of this approach in chapter eight, which looks at the risks that result.

Next we look at the ways that the data collected is analysed and put to use.

i Aldrich, R. (2010) GCHQ The Uncensored History of Britain's Most Secretive Agency, Harper Press, London
ii http://www.spiegel.de/international/europe/british-spy-agency-gchq-hacked-belgian-telecoms-firm-a-923406.html
iii https://firstlook.org/theintercept/2014/12/13/belgacom-hack-gchq-inside-story/
iv GCHQ and the NSA have targeted EU officials through their access to data, as we show elsewhere in this report.
v https://firstlook.org/theintercept/2014/11/24/secret-regin-malware-belgacom-nsa-gchq/
vi http://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
vii https://firstlook.org/theintercept/2015/02/19/great-sim-heist/
viii http://electrospaces.blogspot.co.uk/2015/02/nsa-and-gchq-stealing-sim-card-keys-few.html
ix http://www.spiegel.de/international/germany/gchq-and-nsa-targeted-private-german-companies-a-961444.html
x http://www.spiegel.de/international/world/snowden-documents-indicate-nsa-has-breached-deutsche-telekom-a-991503.html
xi https://www.torproject.org/about/torusers.html.en
xii https://en.wikipedia.org/wiki/Tor_%28anonymity_network%29
xiii http://www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document
xiv http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document
xv http://daserste.ndr.de/panorama/aktuell/nsa230_page-1.html
xvi https://firstlook.org/theintercept/document/2014/03/12/industrial-scale-exploitation/
xvii http://www.wired.com/2013/09/nsa-router-hacking/
xviii https://www.gov.uk/government/consultations/interception-of-communications-and-equipment-interference-draft-codes-of-practice
xix https://firstlook.org/theintercept/document/2014/03/12/thousands-implants/
xx 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
xxi http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-Internet.html?_r=1
xxii https://firstlook.org/theintercept/document/2014/03/12/nsa-gchqs-quantumtheory-hacking-tactics/
xxiii https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html
xxiv http://www.spiegel.de/media/media-35660.pdf
xxv https://firstlook.org/theintercept/document/2014/03/12/five-eyes-hacking-large-routers/
xxvi http://www.spiegel.de/netzwelt/netzpolitik/quantumtheory-wie-die-nsa-weltweit-rechner-hackt-a-941149.html
xxvii https://www.aclu.org/files/natsec/nsa/menwith-hill-station-leverages-xkeyscore-for.pdf
xxviii http://notes.rjgallagher.co.uk/2013/12/gchq-quantum-hacking-surveillance-legality-nsa-sweden.html
xxix 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
xxx https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/
xxxi https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html
xxxii https://robert.sesek.com/2014/9/unraveling_nsa_s_turbulence_programs.html
xxxiii https://firstlook.org/theintercept/2014/03/12/nsa-plans-infect-millions-computers-malware/
xxxiv https://nex.sx/blog/2015-01-27-everything-we-know-of-nsa-and-five-eyes-malware.html
xxxv http://www.spiegel.de/media/media-35688.pdf
xxxvi http://www.spiegel.de/media/media-35662.pdf
xxxvii https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0129/4a1e88b7.dir/doc.pdf
xxxviii http://securelist.com/blog/research/68525/comparing-the-regin-module-50251-and-the-qwerty-keylogger/
xxxix http://www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html

xl http://masssurveillance.info/
xli http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
xlii http://www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html
xliii http://www.spiegel.de/international/germany/bild-1010361-793524.html
xliv https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH01f2/4d5034e3.dir/doc.pdf
xlv http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
xlvi See Interception Capabilities 2000 report referenced in the previous section
xlvii http://www.reuters.com/article/2014/03/31/us-usa-security-nsa-rsa-idUSBREA2U0TY20140331
xlviii http://www.cnet.com/uk/news/feds-put-heat-on-web-firms-for-master-encryption-keys/
xlix http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security
l http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/
li http://securityaffairs.co/wordpress/14561/malware/zero-day-market-governments-main-buyers.html
lii http://www.spiegel.de/media/media-35660.pdf
liii http://heartbleed.com
liv http://www.bloomberg.com/news/2014-04-11/nsa-said-to-have-used-heartbleed-bug-exposing-consumers.html
lv http://www.bloomberg.com/news/2013-06-14/u-s-agencies-said-to-swap-data-with-thousands-of-firms.html
lvi http://www.spiegel.de/media/media-35512.pdf
lvii http://www.spiegel.de/media/media-35509.pdf