MEDIANZ • VOL 14 NO 2 • 2014
DOI: http://dx.doi.org/10.11157/medianz-vol14iss2id119

- KEYNOTE -

Surveillance and Privacy in the Snowden Era

Nicky Hager

Introduction

The purpose of this paper is to give an overview of issues of mass surveillance, the subject that Edward Snowden has so spectacularly brought to world attention. Many readers will have been following the revelations closely, but general public understanding seems fairly confused and imprecise. Indeed, popular understanding of the Snowden revelations amounts to something like: 'Everyone is being spied on all the time', while the typical talk back radio host reply is: 'I don't care if someone spies on me. If you've done nothing wrong, you've got nothing to hide'. There is also a perception that 'It's always gone on' and 'everyone does it anyway'. All of these positions are wrong.

I believe the more accurately we understand the issues of surveillance and privacy, the more clearly we can see where the harm is, what needs to change and how to effect this change. I will be discussing the history of electronic surveillance, the origins and growth of mass surveillance systems, what the Snowden leaks have revealed and their impact on the Internet and privacy. Finally I will discuss what we can do about it.

Lessons from the history of electronic surveillance

The Anglo-American spying system dates from WWII and was then put on a permanent footing in the late 1940s as part of the Cold War. A system of radio eavesdropping stations was dotted around the world as part of the intelligence war between the superpowers.

The US National Security Agency led the system, assisted by Britain and three of its former colonies: Australia, Canada and New Zealand. This is when New Zealand became embedded in the US-run electronic eavesdropping alliance, doing what they call 'signals intelligence', the work of the New Zealand GCSB (Government Communications Security Bureau). One of the secret signals intelligence stations was in New Zealand: an isolated group of top secret staff in a building next door to Navy communications at Irirangi, just

Nicky Hager is an author and investigative journalist based in Wellington, New Zealand. He has written five best-selling books and specializes in investigating hard-to-document subjects, such as the military, intelligence agencies and public relations.

south of Waiouru. Staff who worked at the station told me about how they received their daily orders from Australia or sometimes from a US centre in Japan and were given remote tasks such as tuning in to a Soviet troop movement in Siberia. Some of these staff were also posted to work in a UK-run station in Singapore during the Vietnam War helping provide targets in Vietnam and surrounding countries; and more again worked in shifts in a secret facility in Melbourne that was connected to eavesdropping radio antennae on Hong Kong island and helped spy on China. It was all totally secret and was perhaps our deepest signals intelligence involvement in the Cold War.

At that stage the NSA and allies like New Zealand were mainly targeting militaries, governments, international organisations—part of an obsessive interest in the Soviet Union and other communist countries by the US and Britain. However, as the Cold War eased the system was not cut back. Increasingly these agencies were instead redirected to target virtually every country on earth, friend or foe. The world was divided up geographically between the allies (for example, the New Zealand region stretches from French Polynesia to the Solomons) and New Zealand also joined in alliance wide projects.

For New Zealand, a striking feature is that most targets had nothing to do with national security—the usual justification for the powers given to intelligence agencies. Instead, as I interviewed GCSB staff, I found that the main preoccupations were trade talks, Japan, all Pacific island countries, the United Nations and so on. The secret GCSB annual report for 1986 listed its main targets for the year, including French Antarctic communications, Vietnamese diplomatic, North Korean diplomatic, Egyptian diplomatic and Argentine naval for the British, East German diplomatic, Japanese diplomatic, Philippine diplomatic, South African Armed Forces, Laotian diplomatic and UN diplomatic.

David Lange's Labour Government was helping the Allies spy on the UN and indeed the GCSB still continues to do so. The targeting comes mostly from the Allies and frequently seems inconsistent with New Zealand international policy and values. It was nothing like the WWII period in which the alliance began, which involved dire national security threats. New Zealand was simply helping its old allies to promote their economic, diplomatic and military interest around the world. But the claimed focus on national security allowed special privileges. Hardly anyone in government or elsewhere knew anything about its operations, normal systems of government and democratic control did not apply.

The era of the first mass surveillance systems: late 1970s and 1980s

I learned about New Zealand's role in mass surveillance systems because I made the GCSB one of my research interests and eventually interviewed staff in many areas of the organisation. The most important things they described concerned their super-secret intelligence collection system called Echelon. Echelon was based on a new principle. Rather than targeting a particular person or radio transmitter, it was designed to intercept whole flows of the world's communications—everything, and then search through the communications for intelligence.

The New Zealand Echelon station intercepts normal commercial communications satellites (see Figure 1). The satellite signals are broken down into individual e-mails, faxes, phones calls etc. (See Figure 2). These are run through 'Dictionary' computers that search for 'keywords' (also called selectors) such as a name or e-mail address, and all messages containing these keywords are copied and sent to the intelligence agency headquarters (See Figure 3). Most keyword targets at Waihopai originate from US and other allies, and the resulting intercepted communications are sent straight back to the requesting agency (See Figure 4). As the manuals inside the station show, the target satellites are international communications satellites (See Figure 5). I used the information given by the NZ staff to document the network of sister stations around the world. Figure 6, for instance, is a Waihopai-like satellite interception station at Yakima in the North-western United States, and Figure 7 shows an interception base at Misawa in Japan. The result of this research was my book Secret Power (Figure. 8), published in 1996, which has had an extraordinary amount of overseas publicity. This continues: in January 2014 an updated version of the book was launched in Arabic in Cairo.

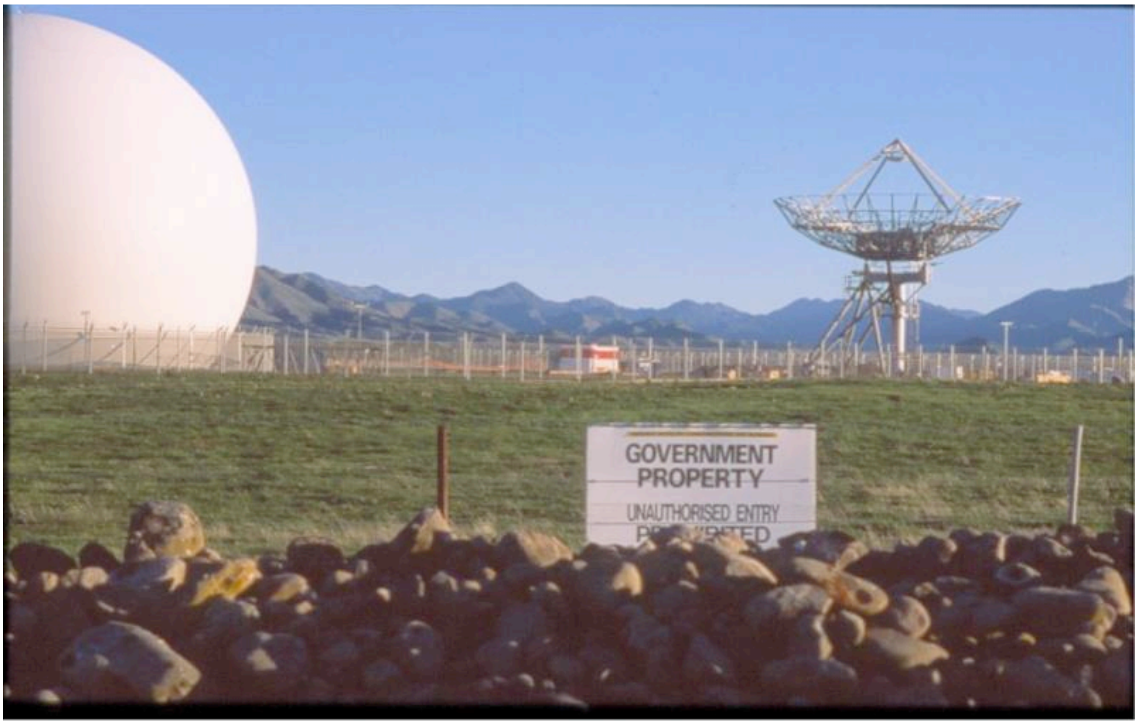


Figure. 1: The New Zealand Echelon Station. (Photo by author)

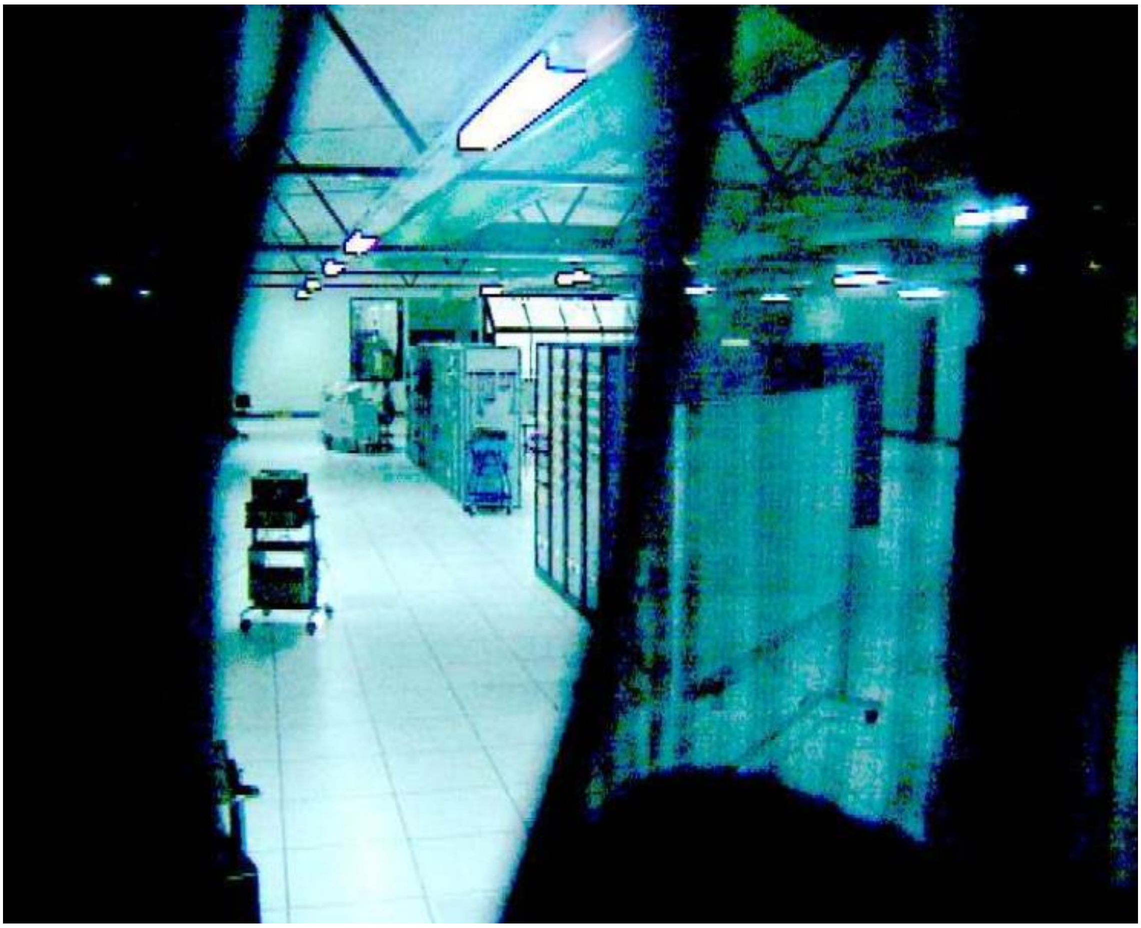


Figure 2: Signal processing equipment inside the New Zealand Echelon Station. (Photo by author)

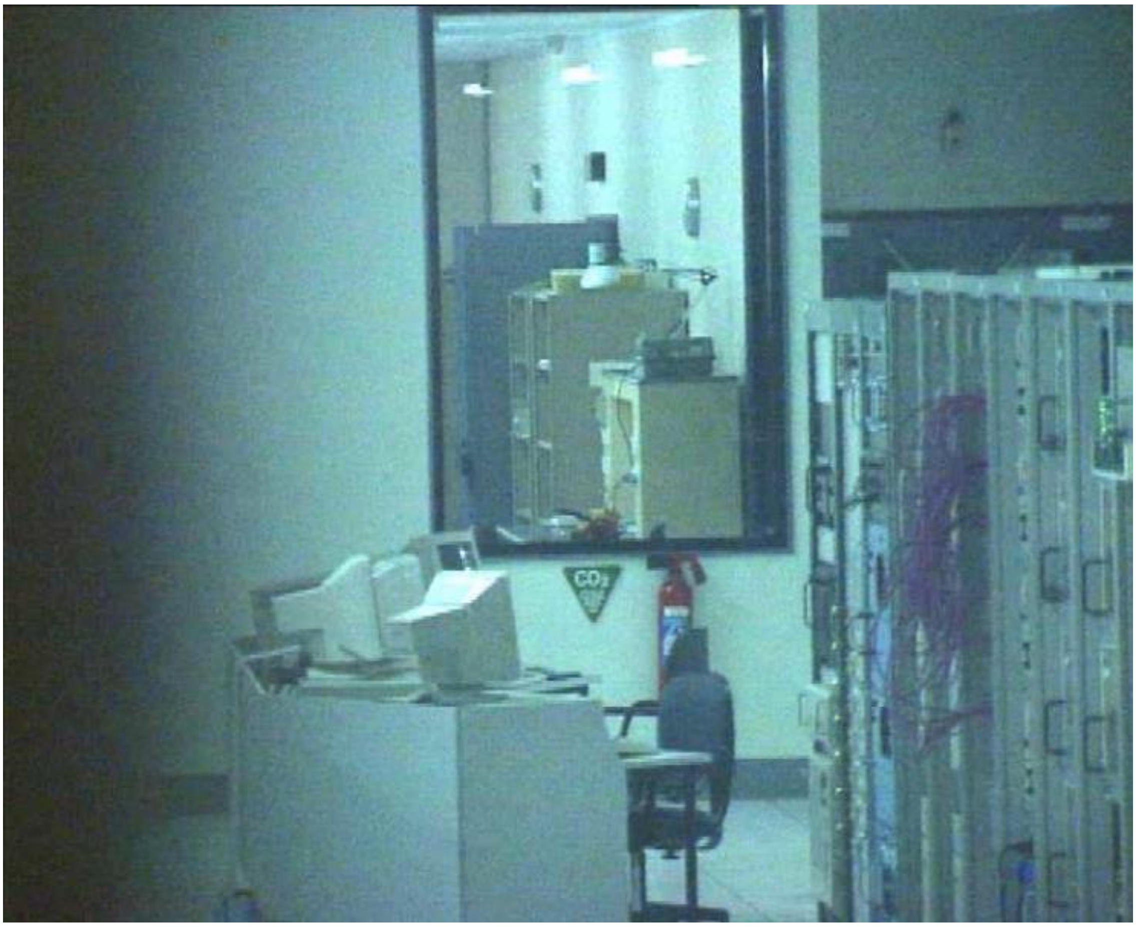


Figure 3: 'Dictionary' computers inside the New Zealand Echelon Station. (Photo by author)

Figure 4: Workstations for keyword targeting. (Photo by author)

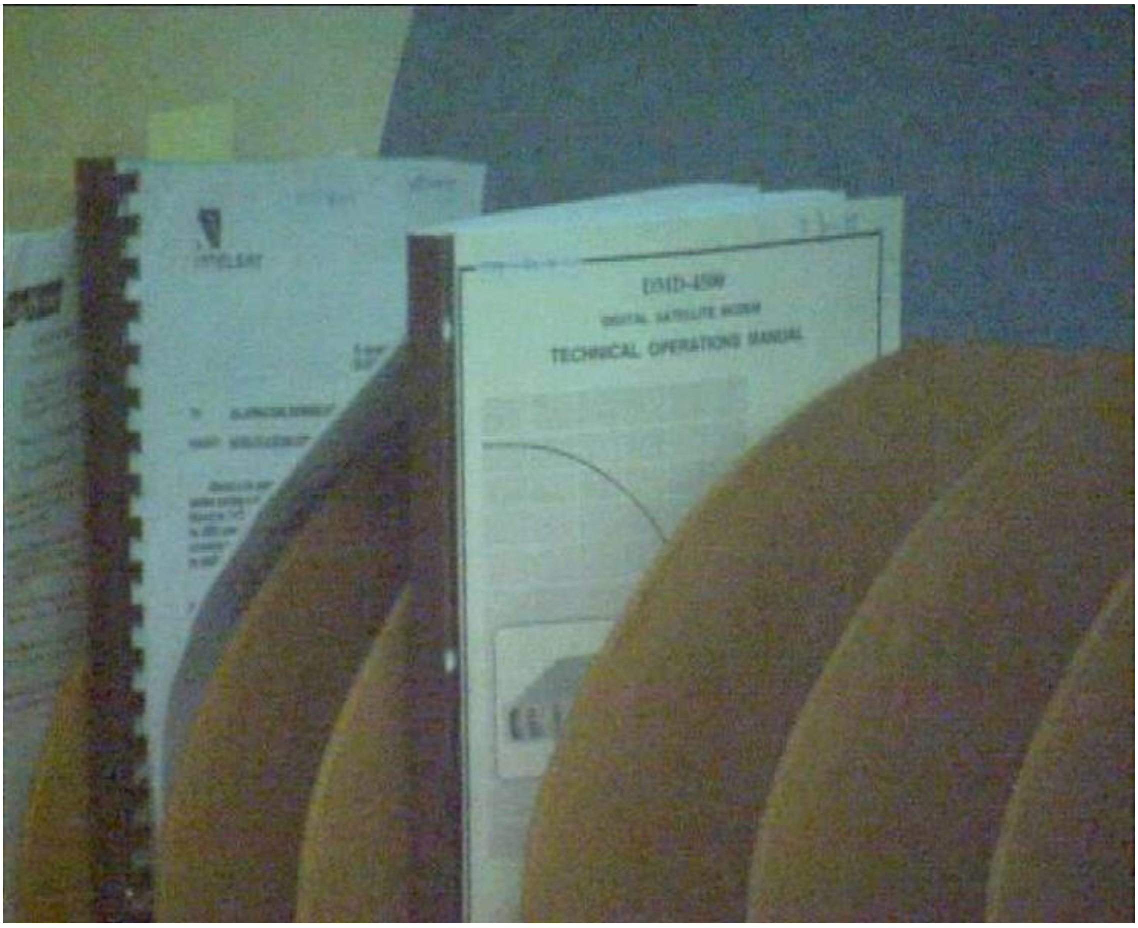


Figure 5: Manuals for Intelsat satellite operations. (Photo by author)

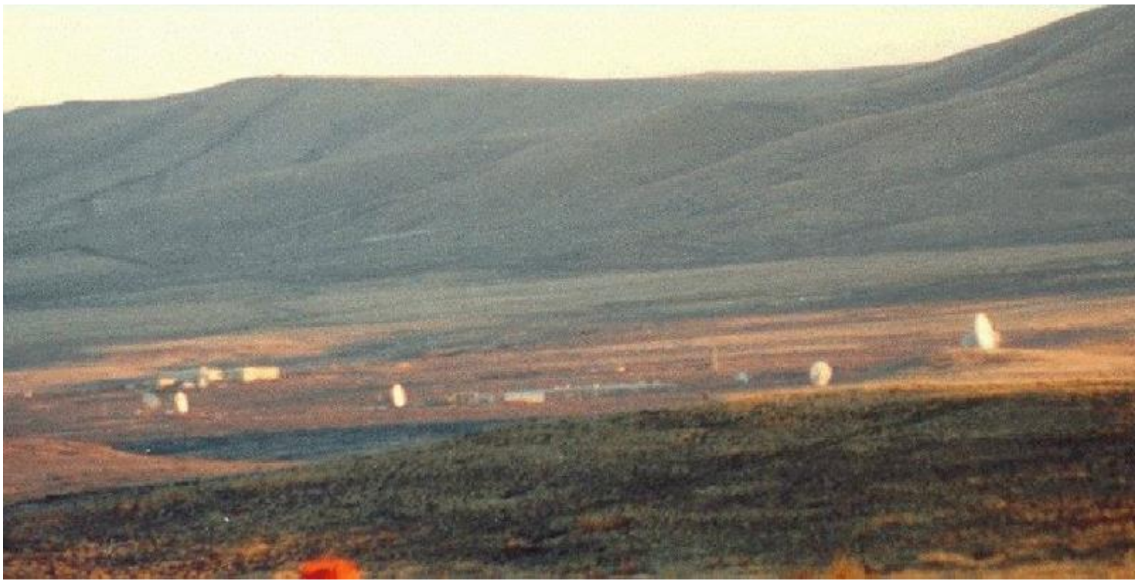


Figure 6: Echelon station in Yakima, United States. (Photo by author)

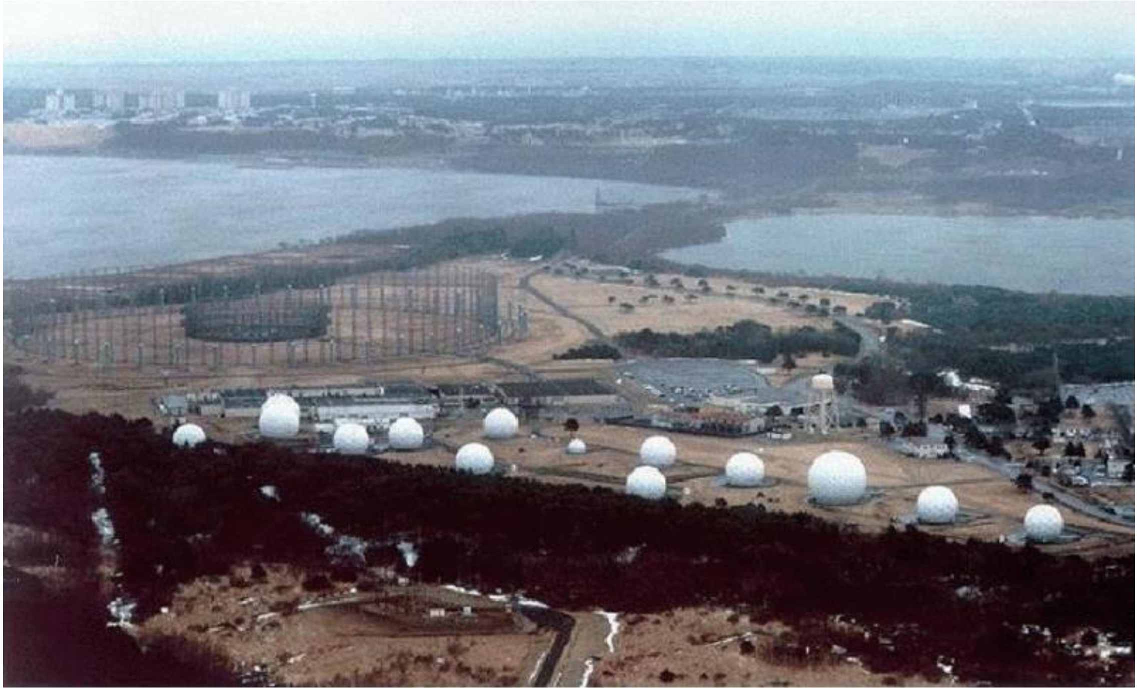


Figure 7: Echelon station in Misawa, Japan. (Photo by author)

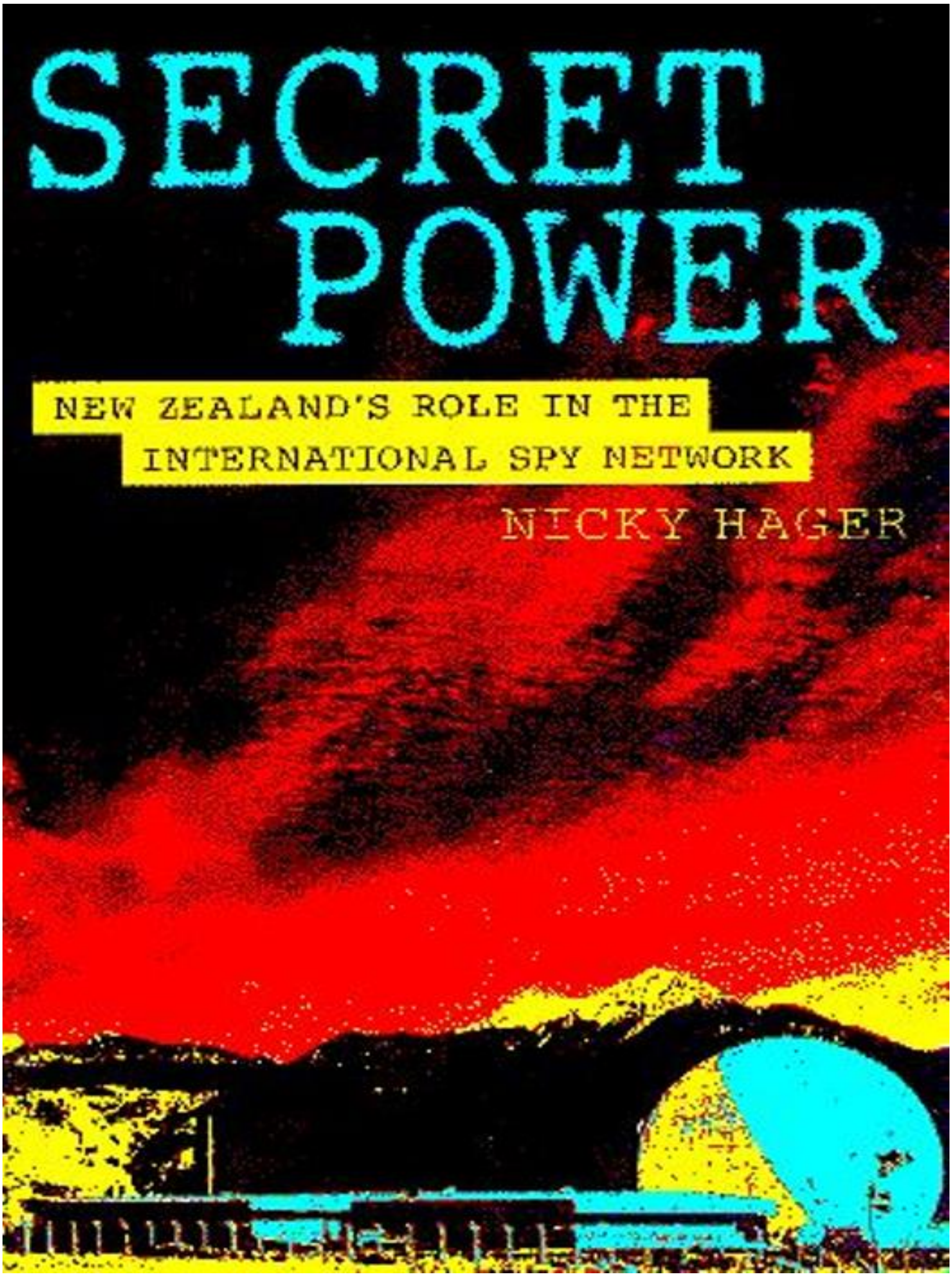


Figure 8: Cover of *Secret Power*. (Image courtesy of author)

It is significant that the world's first detailed knowledge of mass surveillance systems came from New Zealand intelligence whistleblowers. The book *Secret Power* was featured two years after its release in a European Parliament report that concluded that 'all email, telephone and fax communications are routinely intercepted' (Wright 1998.). It burst into the news in Europe. Headlines read 'Global spy network revealed' and

'Europeans angered by US espionage'. *Le Monde* attacked Britain for using the Government Communications Headquarters (GCHQ) to spy on its European partners, Microsoft was accused of assisting NSA monitoring and the Washington Post reported 'a wave of concern and indignation in Europe' (Hager 2013).

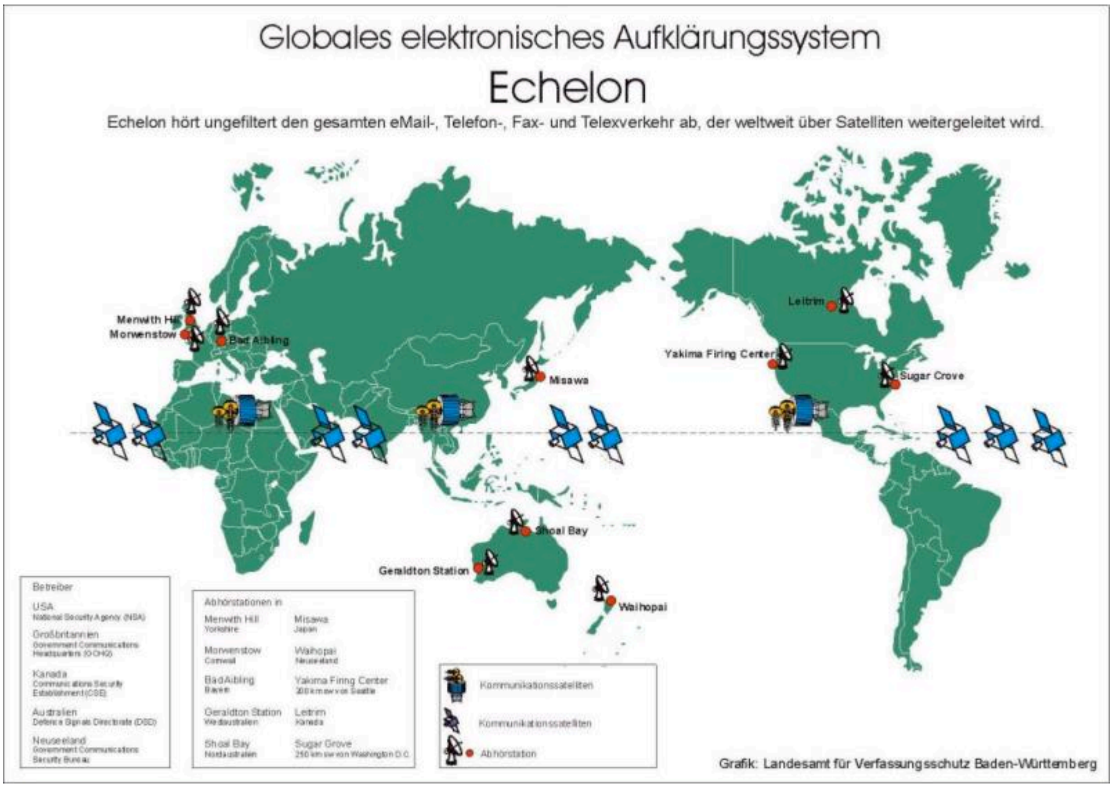


Figure 9: Map of Echelon bases and satellites. (FAS 2010)

These revelations were an important precursor for what has happened since 2013 with the Edward Snowden revelations about mass surveillance. The controversy culminated in a yearlong European Parliament investigation called the 'Temporary Committee on the ECHELON Interception System.' The Echelon committee report recommended radical proposals for the countries of Europe to protect themselves from Anglo-American surveillance, including that they 'promote, develop and manufacture European encryption technology' for all citizens and European institutions. It urged all European Union member countries to:

- Acknowledge the existence of Echelon system
- Inform their citizens about the threats to privacy
- Establish Europe-wide advisory agencies to provide practical assistance in protection against surveillance, including promoting encryption technology and development of open-source encryption software.
- Systematically encrypt their government e-mails 'so that ultimately encryption becomes the norm'. (European Parliament 2001)

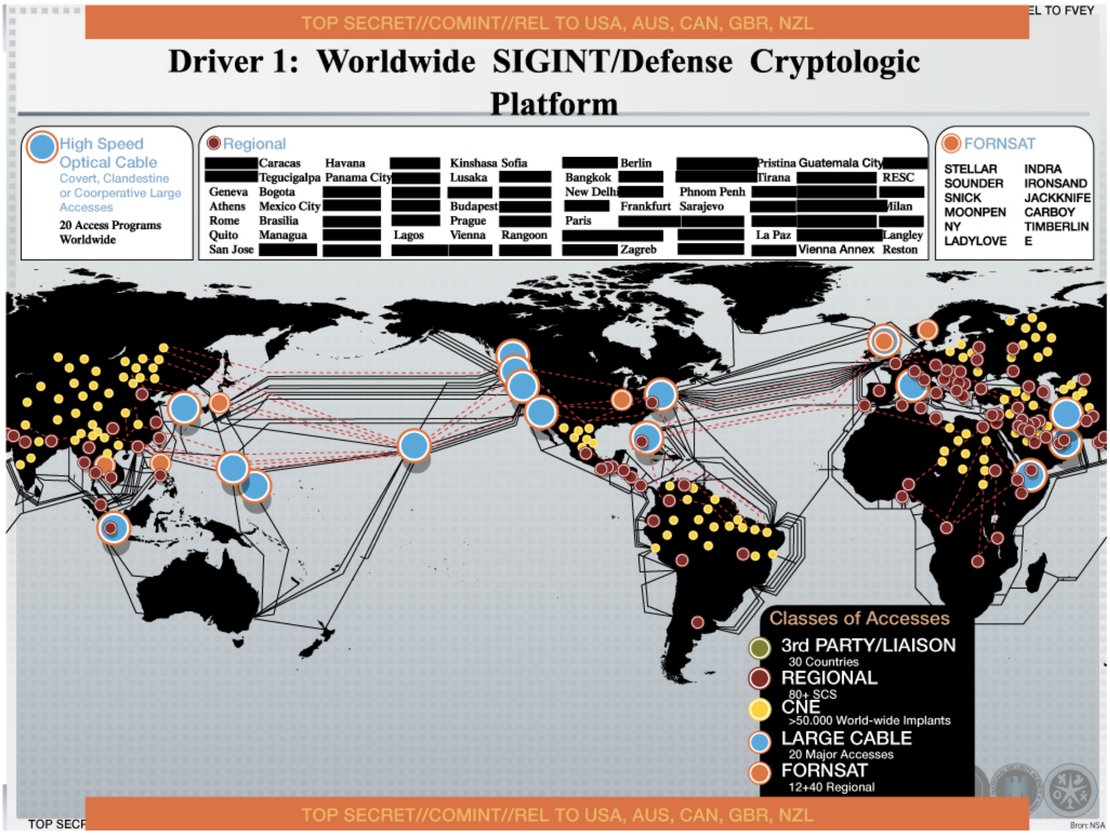
It all looked very promising. And then, as Alan Bennett wrote in *The History Boys* (2006), 'history rattled over the points'. The report was presented to full European Parliament on the fateful date, 5 September 2001. Four days later the issue was completely swept away. Instead of improvement, things all got worse.

Three factors coincided to produce the enormous expansion of surveillance we've seen in the new century. First, the War on Terror has led to a huge expansion of powers and resources for intelligence services, with fewer restraints and compliant political leaders. Second, developments in telecommunications and the Internet led to people and organisations spending larger and larger parts of their professional and personal lives on computers and the online. Third, advancements in digital technology allowed the creation of previously unimaginable spying systems. These three factors combined over a very short period to enable the scale of mass surveillance we have today.

Mostly these surveillance developments were occurring in secret, but there is a fourth historic factor. Julian Assange had an idea, borne in the context of the invasion of Iraq and secrecy and repressiveness of the War on Terror years. (I should explain that I regard Julian as a friend and don't separate him and Wikileaks.) The idea was that leaking in the digital age provided a powerful way to counter excesses and abuses of power. I remember when Julian was first starting Wikileaks from Australia in 2006, with no one taking him very seriously. By pure hard work and force of personality he built the idea over the following years. This idea inspired Chelsea Manning whose actions, I believe, probably inspired Edward Snowden. This is how ideas change the world.

With Snowden's leaks, the wheel has turned full circle and worldwide debate on mass surveillance is back to and stronger than it was before the War on Terror. What have Edward Snowden's leaks revealed? They show several distinct components within today's mass surveillance systems.

First, Snowden has revealed the expansion of the Echelon system. Again, this involves attempting to intercept indiscriminately all the bulk communications flows between and within countries—everything, and then search it for intelligence targets. When I wrote about Echelon, the main technology for bulk communication between countries was satellites, so these were the focus of the surveillance. Today fibre optic cables provide the high capacity trunk routes of the Internet and telecommunications. The modern version of the Echelon system targets all the fibre networks as well as the satellite communications. Figure 10 below is a NSA map released by Edward Snowden showing the surveillance system in 2013. The orange dots are satellite interception stations like Waihopai. The blue dots are underseas cable interception operations and the 'Regional' red dots show interception units hidden inside US and allied embassies in capital cities around the world.



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

EL TO FVEY

Driver 1: Worldwide SIGINT/Defense Cryptologic Platform

High Speed Optical Cable
Covert, Clandestine or Coorperative Large Accesses
20 Access Programs Worldwide

Regional
[redacted] Caracas Havana [redacted] Kinshasa Sofia [redacted] Berlin [redacted] Pristina Guatemala City [redacted]
[redacted] Tegucigalpa Panama City [redacted] Lusaka [redacted] Bangkok [redacted] [redacted] Tirana [redacted] RESC
Geneva Bogota [redacted] [redacted] [redacted] [redacted] New Delhi [redacted] Phnom Penh [redacted] [redacted] [redacted]
Athens Mexico City [redacted] [redacted] Budapest [redacted] [redacted] Frankfurt Sarajevo [redacted] [redacted]ilan
Rome Brasilia [redacted] [redacted] Prague [redacted] Paris [redacted] [redacted] [redacted] [redacted] [redacted]
Quito Managua [redacted] Lagos Vienna Rangoon [redacted] [redacted] La Paz [redacted] Langley
San Jose [redacted] [redacted] [redacted] [redacted] [redacted] [redacted] Zagreb [redacted] [redacted] Vienna Annex Reston

FORNSAT
STELLAR INDRA
SOUNDER IRONSAND
SNICK JACKKNIFE
MOONPEN CARBOY
NY TIMBERLIN
LADYLOVE E

Classes of Accesses
● 3rd PARTY/LIAISON
30 Countries
● REGIONAL
80+ SCS
● CNE
>50.000 World-wide Implants
● LARGE CABLE
20 Major Accesses
● FORNSAT
12+40 Regional

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

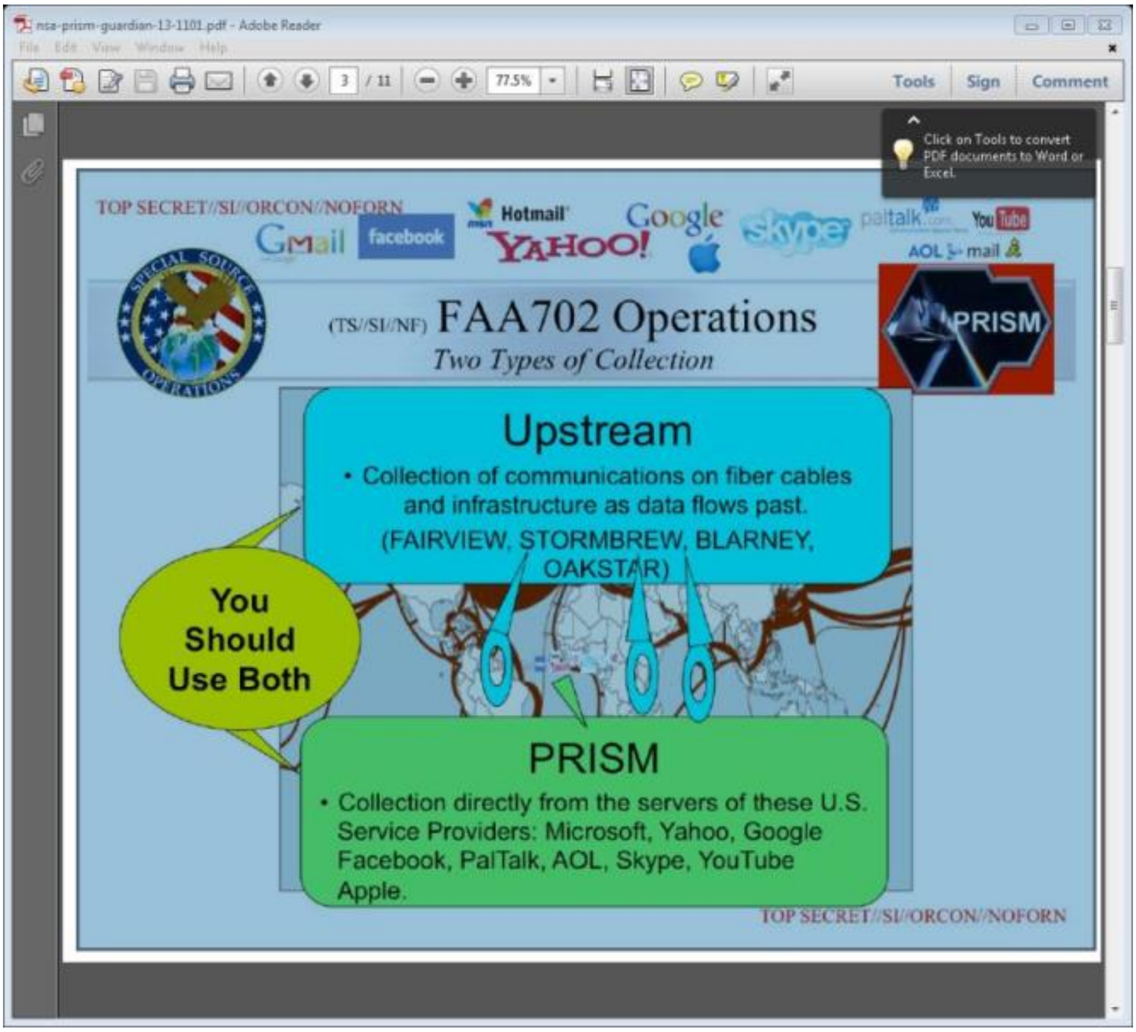
TOP SECR

Bron: NSA

Figure 10: Global surveillance system as of 2013. (Snowden 2013)

The second major component is PRISM, which tends to get muddled with other bulk capture systems but is quite different. It is an FBI-developed system. Starting in the mid-1990s, the FBI pushed country by country for the adoption of standardised laws and systems for monitoring telecommunications networks. There are now laws in many countries requiring all Internet and telecommunications companies to install 'interception capable' equipment and allow intelligence agencies access, usually under a warrant. In New Zealand, for example, I've written about the systems built into the Telecom and other networks (Hager 2010.) This is what TICS bill is about: it means Telecommunications Interception Capability—that is, having the capability built in.

Snowden's revelations about interception of Gmail, Facebook and Microsoft are about intelligence agencies using this built-in intercept capability—and then bending or breaking the law to suck up bulk metadata from these companies for use in intelligence searches. These operations are called Special Source Operations. See, for example, how this NSA training slide (Figure 11) advises operators that they have two different options for targeting: searching the bulk intercept (e.g. satellite interception and underseas cable interception) or going directly to one of the big Internet companies located helpfully on US soil (via PRISM).



nsa-prism-guardian-13-1101.pdf - Adobe Reader
File Edit View Window Help
3 / 11
77.5%
Tools
Sign
Comment
Click on Tools to convert PDF documents to Word or Excel.
SPECIAL SOURCE OPERATIONS
PRISM

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) FAA702 Operations

Two Types of Collection

Upstream

- Collection of communications on fiber cables and infrastructure as data flows past. (FAIRVIEW, STORMBREW, BLARNEY, OAKSTAR)

You Should Use Both

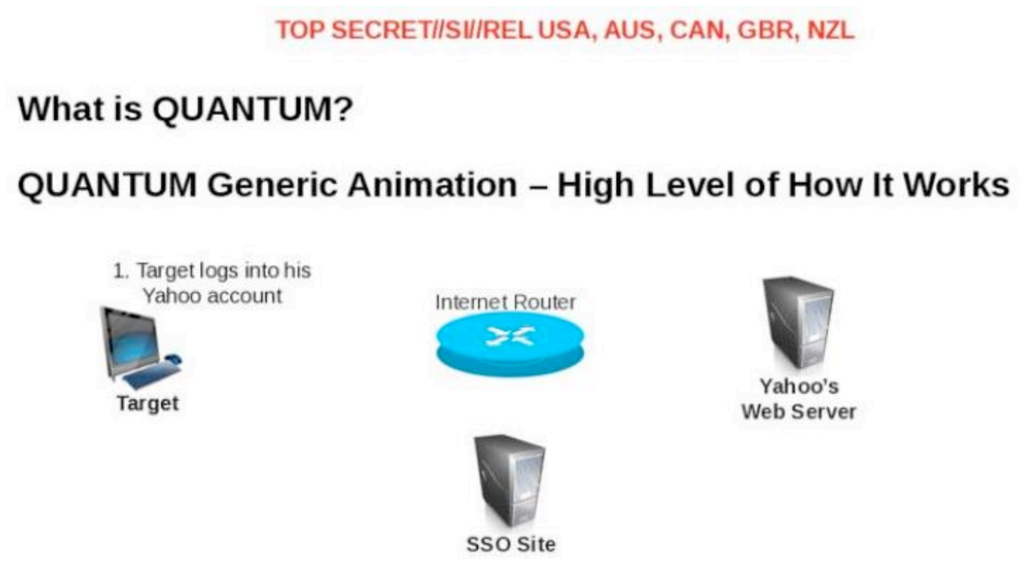
PRISM

- Collection directly from the servers of these U.S. Service Providers: Microsoft, Yahoo, Google Facebook, PalTalk, AOL, Skype, YouTube Apple.

TOP SECRET//SI//ORCON//NOFORN

Figure 11: NSA Training Slide. (Ball 2013)

The third major component of the surveillance system is computer hacking (usually referred to as ‘cyber warfare’, but actually it's cyber spying). This is the least known area and the one that shocked me most in Snowden's revelations. These agencies now have sophisticated programmes for breaking into computers of, for instance, target individuals, foreign government agencies or telecommunications companies to get at their clients. Figures 12-18 below are from another NSA training presentation showing an example of how the hacking can work. In this case, it targets someone logging into their Yahoo e-mail account.



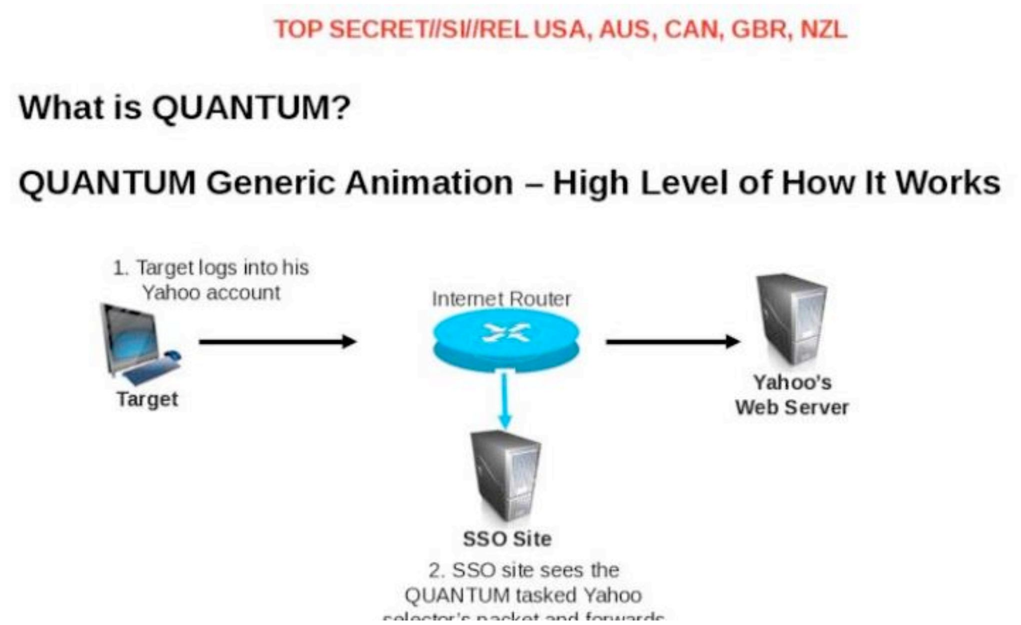
TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

1. Target logs into his Yahoo account

Figure 12: the target person logs into Yahoo. (Texas Cryptologic Center)



TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

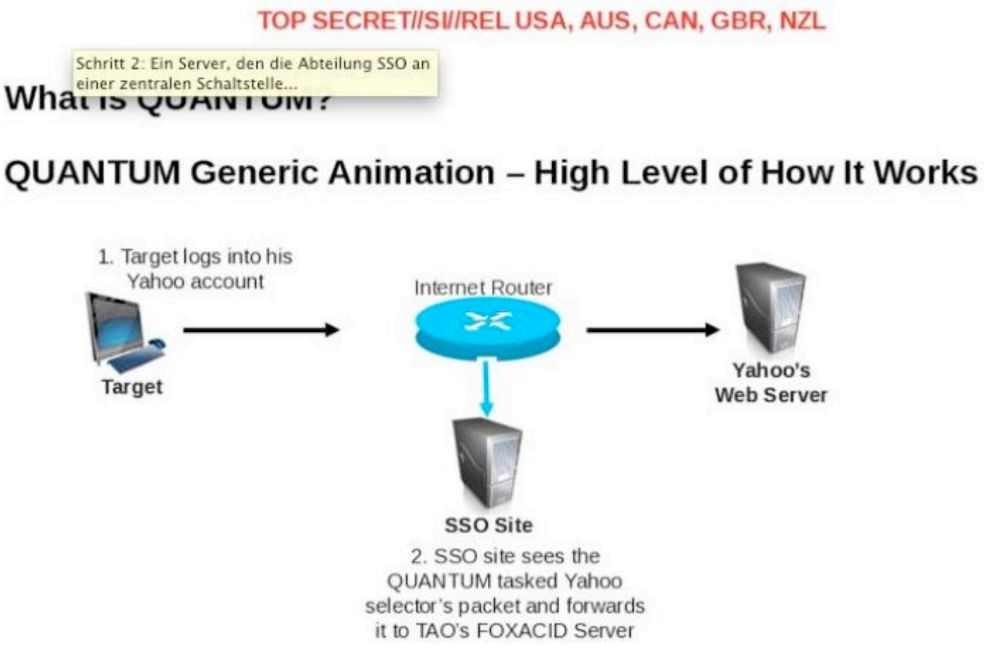
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

1. Target logs into his Yahoo account

2. SSO site sees the QUANTUM tasked Yahoo selector's packet and forwards

Figure 13: A SSO Site (special source operations) detects the target user. (Texas Cryptologic Center)



TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

Schritt 2: Ein Server, den die Abteilung SSO an einer zentralen Schaltstelle...

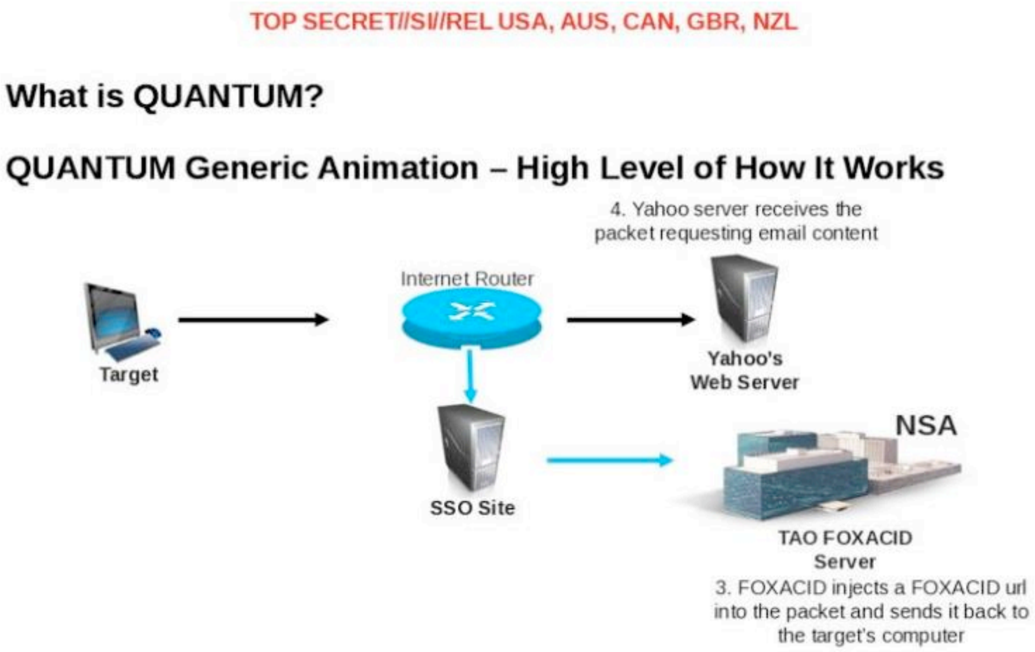
What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

1. Target logs into his Yahoo account

2. SSO site sees the QUANTUM tasked Yahoo selector's packet and forwards it to TAO's FOXACID Server

Figure 14: The target's 'packet' (signals sent to Yahoo) is diverted to the NSA unit called TAO. (Texas Cryptologic Center)



TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

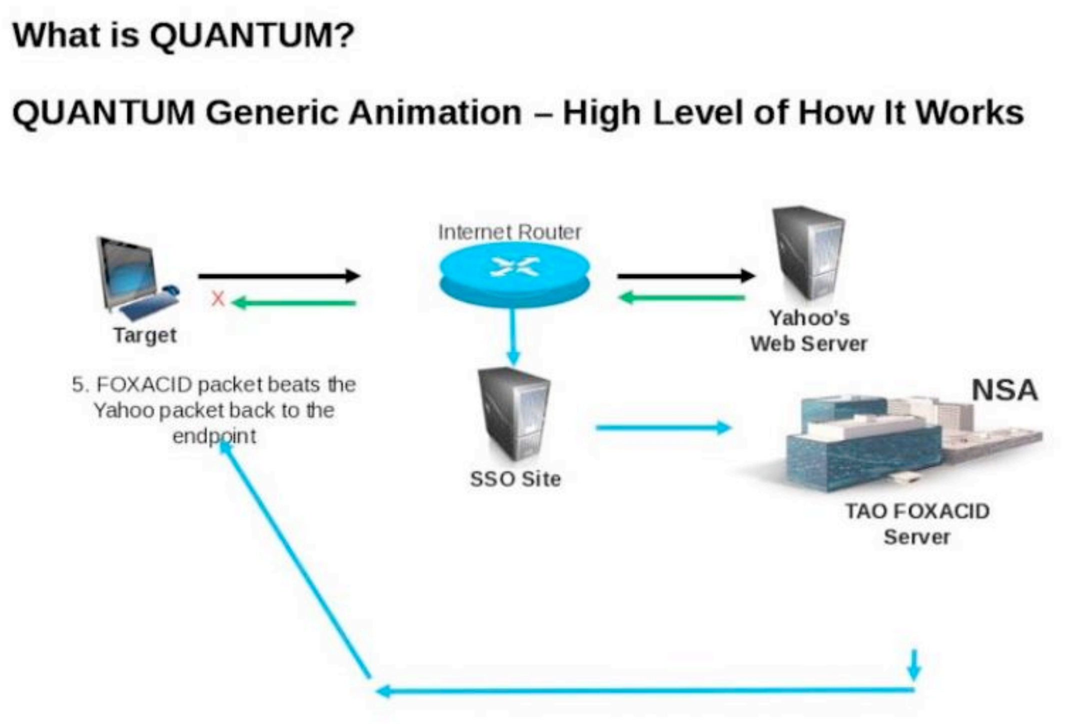
4. Yahoo server receives the packet requesting email content

3. FOXACID injects a FOXACID url into the packet and sends it back to the target's computer

Pasted

Graphic 17.tiff ¬

Figure 15: The NSA's TAO computers inject some computer code into the packet and send it back to the user. (Texas Cryptologic Center)

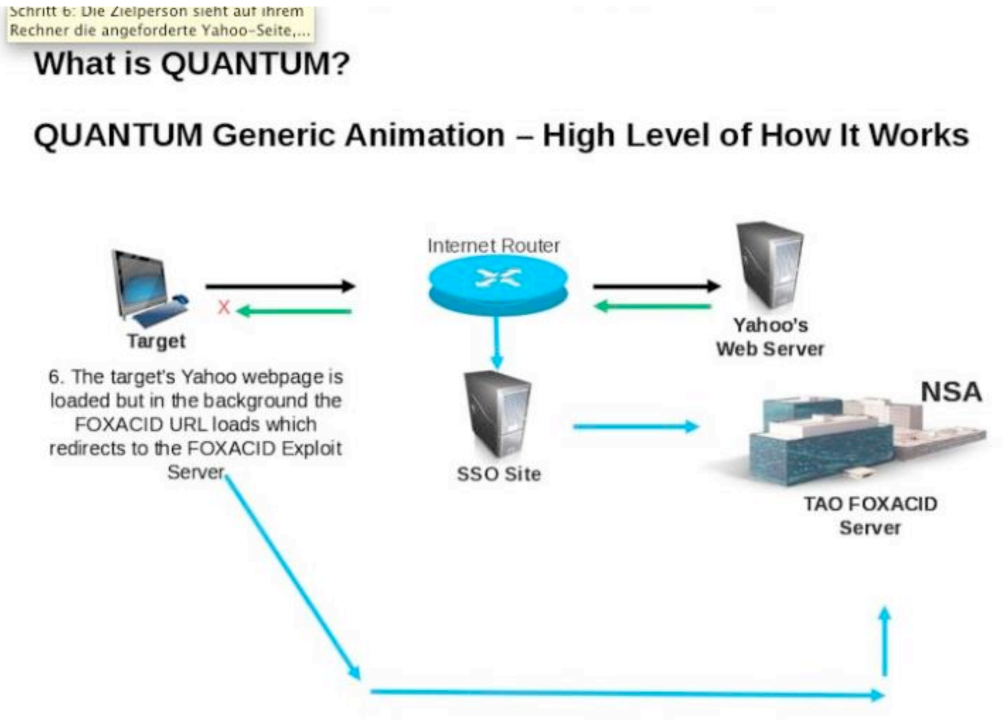


What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

5. FOXACID packet beats the Yahoo packet back to the endpoint

Figure 16: The NSA's 'Foxacid" code beats the real Yahoo reply back to the target's computer. (Texas Cryptologic Center)



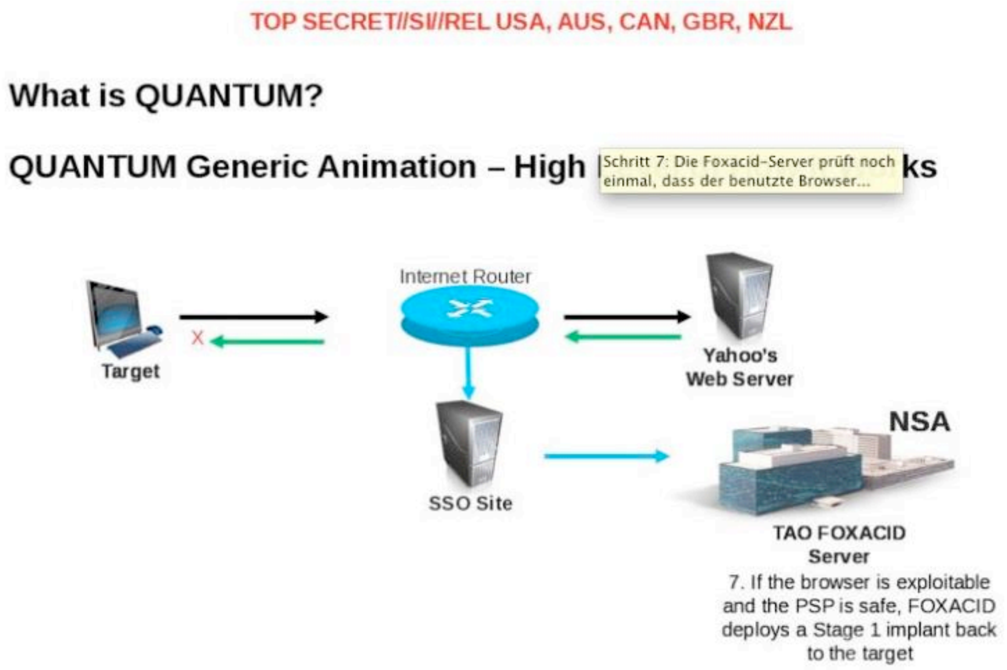
Schritt 6: Die Zielperson sieht auf ihrem Rechner die angeforderte Yahoo-Seite,...

What is QUANTUM?

QUANTUM Generic Animation – High Level of How It Works

6. The target's Yahoo webpage is loaded but in the background the FOXACID URL loads which redirects to the FOXACID Exploit Server

Figure 17: The Foxacid software now works in the background of the Yahoo webpage. (Texas Cryptologic Center)



TOP SECRET//SI//REL USA, AUS, CAN, GBR, NZL

What is QUANTUM?

QUANTUM Generic Animation – High Schritt 7: Die Foxacid-Server prüft noch einmal, dass der benutzte Browser... ks

Internet Router

Target

X

Yahoo's Web Server

NSA

SSO Site

TAO FOXACID Server

7. If the browser is exploitable and the PSP is safe, FOXACID deploys a Stage 1 implant back to the target

Figure 18: The NSA's TAO unit now sends a spying implant into the target user's computer. (Texas Cryptologic Center)

Note that the red writing at the top of the slides shows that this NSA presentation is cleared for release to New Zealanders in the GCSB. New Zealand is an active participant and user of these systems. For example, PRISM and a related system called MARINA appear to have been used to target Kim Dotcom, with the GCSB staff simply asking the American staff at the NSA to do the targeting for them (confidential source).

Just as the American and British agencies spy on friendly nations in Europe, the GCSB spies on friendly countries in the Pacific and Asia: governments, leaders, government agencies, regional and UN offices, and so on. GCSB staff members have also been secretly posted to Afghanistan in targeting roles for over ten years. The GCSB also uses its capabilities to do some work for the New Zealand government, but it is hard to overstate how much of it is tied into the operations of its larger allies. So, as the NSA world map above shows (Figure 10), there are three main components of the NSA surveillance systems: the industrial-scale interception of the world's communications, the targeting of communications companies and the direct hacking of target computers. There are many other parts to this, such as cracking or going around encryption, but these are the main three areas. These mass surveillance systems were being built up over exactly the same years as the Internet was growing (See Figure 19).

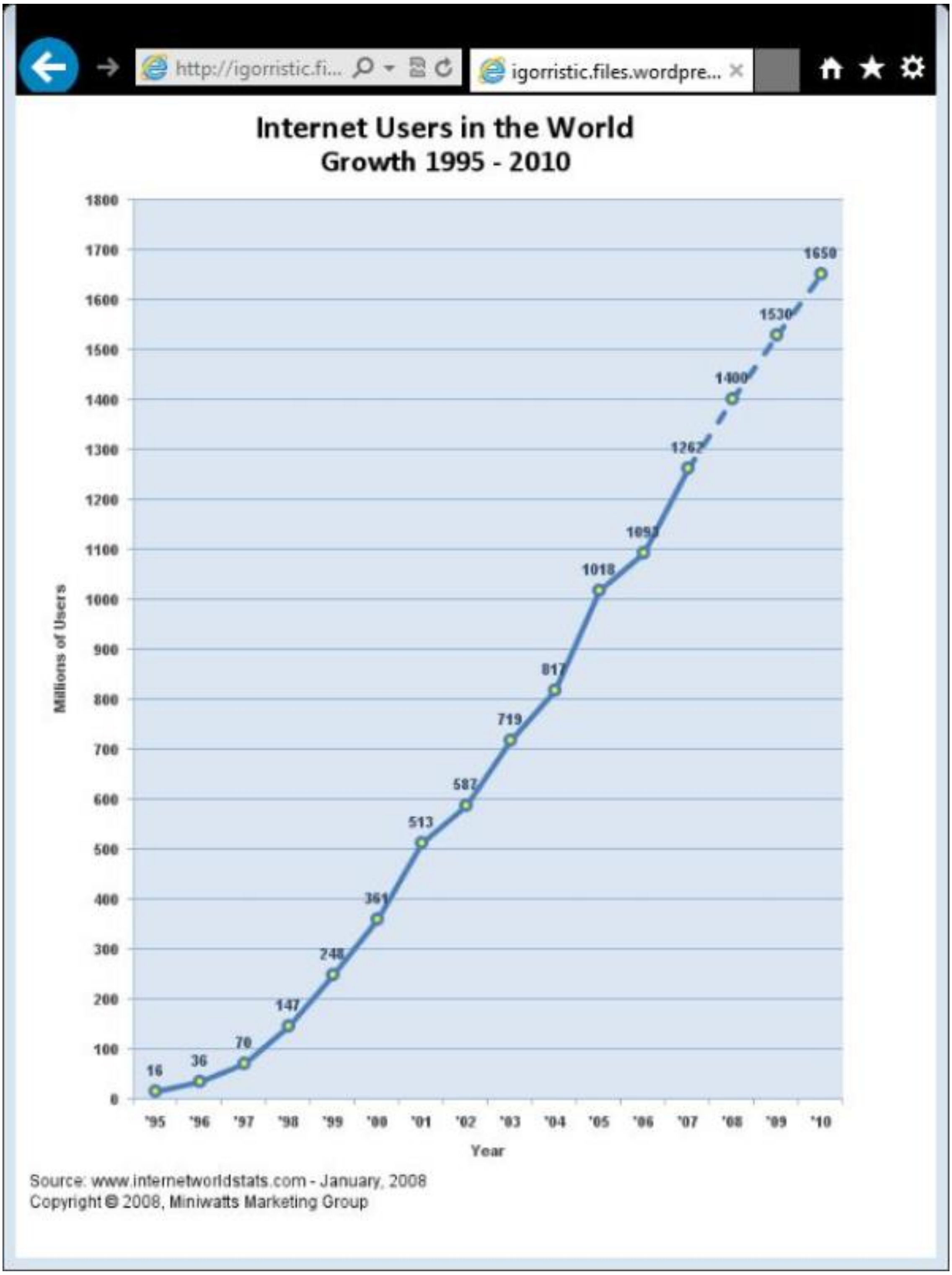
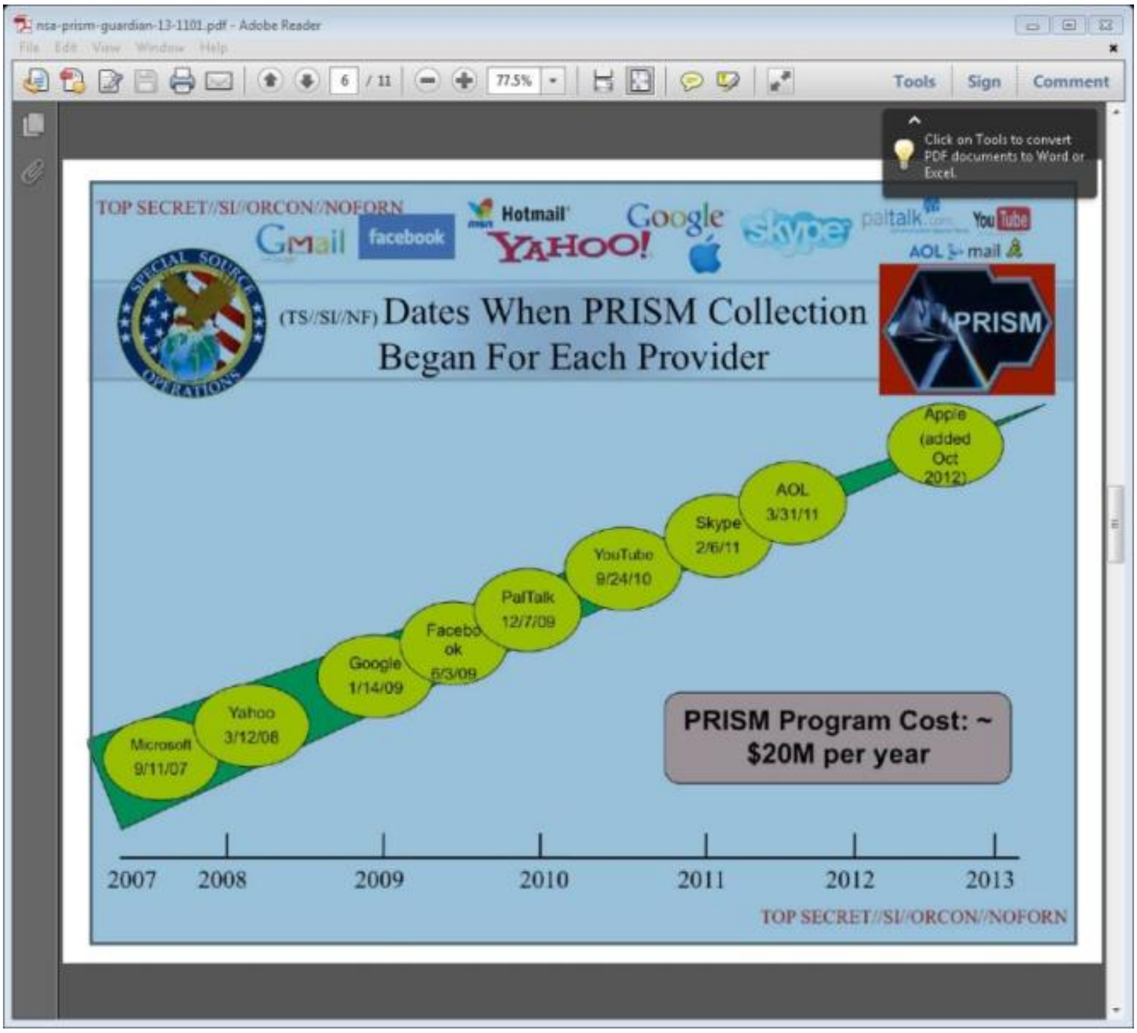


Figure 19: growth in global Internet usage (Miniwatts Marketing Group, 2008)

Indeed, It is staggering how quickly we changed our social lives around the Internet, seeing it as a great global commons where everyone was equal and free. The situation is reminiscent of a joke on the US website The Onion, in March 2011, pre-Snowden. The satirical Onion News Service (ONN) ran a television news item, headed 'CIA's "Facebook" programme dramatically cut Agency's costs' (2011). Newsreader Brooke Alvarez reported: ‘Congress today reauthorised funding for Facebook, the massive on-line surveillance programme run by the CIA. According to Department of Homeland Security reports’, she continued, ‘Facebook has replaced almost every other CIA information gathering programme since it was launched in December 2004’. The report cut to a CIA Deputy Director who told a congressional hearing: ‘After years of secretly monitoring the public, we were astounded that so many people would willingly publicise where they live, their religious and political views, an alphabetised list of all their friends, personal e-mail addresses, phone numbers, hundreds of photographs of themselves, and even status updates of what they were doing moment to moment. It is truly a dream come true for the CIA’. The piece was published two years before the Snowden revelations, which is why it could still feel like satire.

When I interviewed GCSB staff in the 1990s they said they were just overcoming the technical problems of intercepting e-mail. Surveillance has developed rapidly since then. In the first decade of the new century the US and British were installing taps into the world's main underseas cable routes. Then Microsoft agreed to allow NSA access in 2007, Yahoo in 2008, Google in 2009, Skype in 2011 and Apple in 2012 (Figure 20). By around 2009/2010, computer hacking techniques were becoming very sophisticated.



TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) Dates When PRISM Collection Began For Each Provider

PRISM Program Cost: ~ $20M per year

TOP SECRET//SI//ORCON//NOFORN

Figure 20: Dates of PRISM collection for major Internet providers. (Greenwald and MacAskill, 2013)

I believe it is too soon to know what the effect of mass surveillance will be on the Internet. But something like the Internet relies immensely on trust: on ordinary people, organisations, companies and government agencies trusting that their communications and activities are private. This trust has been devastatingly broken.

As many others have asked: why should people ever again trust Internet services located on US soil? Also, it is now clear that the US government used its political muscle to influence technical standards and developments around the world to ensure its intelligence agencies maintained maximum global access. Backdoors and weaknesses built in for the US agencies have weakened the whole system. As US writer Bruce Schneier said: ‘Our choice isn't between a digital world where the NSA can eavesdrop and one where the NSA is prevented from eavesdropping; it's between a digital world that is vulnerable to all attackers, and one that is secure for all users’ (2014). I now want to turn attention back to the privacy issues and after that, what we can do as citizens.

This discussion brings me back to the naïve but familiar response to these issues: the 'I don't care if someone spies on me. If you've done nothing wrong, you've got nothing to hide' attitude. This is the usual East Germany-style excuse for surveillance, but the joke is that the people who use this argument would actually be deeply shocked and concerned if they discovered they were being spied on.

Privacy is a subtle idea but it is fundamental to our sense of self and well-being. It is about preserving the space to have a self. Our rightful privacy includes all our private hopes and dreams, our fears, doubts or guilty secrets, the things we're embarrassed about or just don't want others to know, the health or family problems that are no one else's business but might lose us our job, the different faces we choose to wear in different situations, our business secrets or political tactics and much more. It is silly to confuse this with hiding criminality. Privacy is very fragile. If people even just fear they are being monitored, then they have already lost freedom and act differently even if they aren't being watched. This is why there have to be very important reasons before allowing surveillance to occur (in one's own country or internationally against others) and especially for turning capabilities that were originally justified for World War-scale threats against people and countries that are not mortal threats. It also means that people like us, who I assume are reading this because they are concerned about issues of privacy and surveillance and want to raise the problems, shouldn't needlessly create fear and uncertainty for ordinary people. I am regularly contacted by people who fear they are being monitored and whose lives and activities are constrained as a result. It's a huge problem.

Accordingly, we should be careful about exaggerated statements such as 'Everyone is being spied on all the time.' Mass surveillance is about capability. It doesn't mean (and it's impossible for it to mean) that more than a tiny proportion of the world's population is being actively monitored. In New Zealand nearly everyone isn't being spied on. In bringing these issues to public awareness, we have a responsibility not to increase the harms that we are concerned about.

What can be done?

The usual answer is that we need better oversight of the intelligence agencies. This wouldn't be worthless, but it is nearly so. Every example in the world shows that oversight of super secret agencies doesn't work and especially in the controversial areas where it's needed most. The answer doesn't lie here. Secrecy is the main obstacle to reform and control of intelligence agencies. Revelations such as Edward Snowden's are generally a very rare event. The normal state of affairs is no information, no debate, no progress, just corrosive non-specific fears. That's why the Wikileaks and Edward Snowden examples are so important.

The first part of the answer to what can be done is that journalists, researchers and whistleblowers need to keep finding a supply of news that holds public attention on these issues and provides impetus for change. We are a small country and everywhere there are people whose former colleagues, or flatmates or cousins work in or have worked in intelligence-related jobs. If that includes you, please seek me out and talk about it.

Second, as a country we need to take security subjects back off 'security experts'. The War on Terror years created legions of well-meaning people who mouthed nonsense such as that the main security threat to New Zealand was terrorism. We need different sorts of policy makers who understand that the best defence for a country like ours is a free and tolerant society with a strong commitment to human rights and the rule of law. This isn't 'namby pamby'. It is the best way of ensuring that we don't become a country blighted by political violence.

Moving on specifically to the Internet, there are many technical responses available to the mass surveillance systems. With good advice and support, these can be implemented at the level of individuals and organizations, providing secure computers, communications and Internet browsing. Yet this is far beyond the technical abilities and awareness of most people and, if left to individuals, 99% of people will never be secure. The real answer lies in government policies designed to protect citizens and organisations: regulations, standards and national systems. This could include an agency called the Government Communications Security Bureau being redesigned to protect the communications security of the country's citizens. More importantly, real progress will come when a coalition of nations comes together to work to provide a secure global Internet: setting up facilities in trusted countries, lobbying on international standards bodies and so on. The leadership for this mostly won't come from the big powers. But there are good precedents for small nations like New Zealand leading the way on issues that end up transforming the world. Examples include the Law of the Sea (which initially would have seemed impossible) and the protection of Antarctica—both of which new Zealanders played leading role in. This sort of collective action is just beginning but it is possible and hopeful. There are also political steps that are needed. Our government could be serious about securing the Internet for all. It could decide that it's not in New Zealand's best interests to spy on friendly countries (which means most countries). It could decide that spying on other countries and citizens can only be justified on strict national security grounds—instantly removing much of the rationale for the GCSB.

Where does New Zealand stand now on these technical, diplomatic and political options? The answer is that they are currently all completely impossible. We need to conclude by understanding the bind that New Zealand is in.

Most New Zealanders would probably applaud New Zealand helping lead a diplomatic effort to build a secure Internet. But New Zealand can't do any of this as things stand. The wishes of both the public and the government are irrelevant. New Zealand's intelligence activities are so utterly integrated into the NSA and other US and British agencies that there is no realistic way that the country could have divergent policies. We cannot back a secure Internet. We cannot offer secure services in NZ (no one would trust them anyway). We can't join multi-lateral efforts. We can't even change our own intelligence agencies operations and targeting. We are in a bind where, as a very small ally, it is basically 'all or nothing' with the US intelligence agencies.

There are thus only two options. We can leave the intelligence alliance, as politely as we can, but obviously not without a cost. In that case many other sorts of relationships with the US and allies could go on, but it would be rocky. Or we can accept that we have no real choice in our national intelligence activities. This reality could be blurred and hidden by secrecy and by minimising political discussion, but the fact would remain that wherever the US and British intelligence agencies went, we would go too. This is the decision that the Snowden revelations raise and that, sooner or later, New Zealand must face.

References

Ball, James. 2013. ‘Slide from Secret PowerPoint Presentation Describes how Program Collects Data “Directly from the Servers” of Tech Firms’. *The Guardian.* 8 June. http://www.theguardian.com/world/2013/jun/08/nsa-prism-server-collection-facebook-google

Bennet, Allen. 2006. *The History Boys.* New York: Faber and Faber.

European Parliament. 2001. *Report PE 305.391, on the Existence of a Global System for the Interception of Private and Commercial Communications (Echelon interception system).* 5 September 2001. http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+REPORT+A5-2001-0264+0+DOC+XML+V0//EN

FAS: Intelligence Resource Program. 2010. ‘Globales Elekronisches Aufklärungssystem’. Last modified 21 October. http://www.fas.org/irp/program/process/echelon.htm

Greenwald, Glenn and Ewen MacAskill. 2013. ‘NSA Prism Program Taps in to User Data of Apple, Google and Others’. *The Guardian*, 7 June. http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data

Hager, Nicky. 2013. ‘Electronic Espionage: 15 years of Inertia’. *Le Monde Diplomatique*, September. http://www.nickyhager.info/electronic-espionage-15-years-of-inertia/

Hager, Nicky. 2010. ‘NZ’s Cyber Spies Win New Powers’. *Sunday Star Times*, 3 January. http://www.nickyhager.info/nzs-cyber-spies-win-new-powers/

Hager, Nicky. 1996. *Secret Power: New Zealand’s Role in the International Spy Network.* Nelson, New Zealand: Craig Potton Publishing.

‘CIA's “Facebook” Program Dramatically Cut Agency's Costs’. 2011. *Onion News Service* video*.* 19 March. http://www.theonion.com/video/cias-facebook-program-dramatically-cut-agencys-cos,19753/

Miniwatts Marketing Group. 2008. ‘Internet Users in the World Growth 1995 – 2010’. January. www.internetworldstats.com

Schneier, Bruce. 2014. 'How the NSA Threatens National Security'. *The Atlantic,* 6 January. http://www.theatlantic.com/technology/archive/2014/01/how-the-nsa-threatens-national-security/282822/

Texas Cryptologic Center. 2015. 'Taylored Access Operations'. Electronic Frontiers Foundation. Accessed 29 January, 2015. https://www.eff.org/document/20131230-spiegel-tao-quantum-theory

'Worldwide SIGINT/Defense Cryptological Platform'. In Support of Edward Snowden: The Courage Foundation. Accessed 4 February 2015, https://edwardsnowden.com/2013/11/23/worldwide-sigintdefense-cryptologic-platform/

Wright, Steve. 1998. 'European Parliament Document PE 166.499, an appraisal of technologies of political control'. Scientific and Technological Options Assessment (STOA). 6 January. http://aei.pitt.edu/5538/