↓

AGAINST THE BLACK BOX

Strategies of Control and Tactics of Resistance

↑

Oliver Smith
Information Experience Design
2014

10,237 Words

↓ Contents

↓ List of Illustrations

0.0 → INTRO-DUCTION

> "If power was previously exerted in the disciplinary practices of design at a built and urban scale, power is shifting into the codes, programs and archives of telecommunications and network technologies."
> - Design Act

As we navigate the network, we step over, round, and through many different systems, services and devices, we connect with some for fractions of a millisecond and others remain with us, in our pockets and about our persons. We put them to work on the information we provide and receive, allowing them to mediate our communications, knowledge and actions, reliant on their inherent capability for data collection, transmission and manipulation. They may seem to be working with us, or for us, but in which direction does the power flow? How can we truly know when it is not possible for us to fully inspect and critique them? They are Black Boxes: we provide an input, they provide an output, but the machinations and manipulations are hidden.

Writing on this topic now, it is necessary to situate discussion firmly in the context of the revelations made by Edward Snowden[1↘] concerning technological data gathering and surveillance programs from the United States' National Security Agency (NSA), the United Kingdom's Government Communications Headquarters (GCHQ) and other security agencies in the 'Five Eyes' program. Revealing, among other things, the widespread collection of internet activity, access

1 http://www.theguardian.com/world/the-nsa-files (Accessed 10th September 2014)

to and the ability to control computer networks and the creation or maintenance of backdoors, or security flaws, in consumer electronics, Snowden's leaks highlighted how little was known about the scale and capabilities of these activities, the potential of many of the consumer devices in daily use to collect and disseminate private information, or be coerced into doing so, and the lack of understanding that even some technology and service providers had of the activities occurring in their own devices and networks. The aim here, then, is to come to an understanding of the structures of power and control that these systems comprise, to investigate existing methods of resistance and dissent, and any shortcomings they may have in the face of this particular expression of power, with a view to outlining and consolidating necessary new counter methods.

We will begin with the origins of the Black Box as a problem solving tool in electrical engineering, and trace its development through military applications to a general structure of knowledge and power, describing a number of specific types of Black Box which will be useful throughout. This will begin to show some of the particular advantages the Black Box holds.

From here, we move to some specific examples of Black Boxes in network and communications technologies, looking at the ways in which they hide their intentions and exert control over their users. These will be linked back to the types of Black Box identified as a way of categorising and identifying their specific natures.

We will then look at some theories that explain some of the ways these exemplary Black Boxes gather and maintain their power, we will look particularly at Strategies, as outlined in Michel de Certeau's 'The Practice of Everyday Life', and the Black Box's implementation of them, as well as ways they consolidate and extend their power beyond this.

From here, with the Black Box pinned down, we can begin to trace methods of resistance, beginning with de Certeau's Tactics, we will look at Tactical Media and some of its shortcomings, moving to the ways in which Critical Engineering addresses these and, using Walter Benjamin's thoughts on the political responsibilities of the author, a way we can bring the myriad methods together to counter the Black Box.

Firstly, let us identify the Black Box. ↵

1.x → THE BLACK BOX

1.0 ↓ The Black Box

During World War II, the mathematician Norbert Wiener worked to improve automatic anti-aircraft targeting systems. Taking the exploratory, electrical-engineering approach of black box analysis and applying it to human behaviour, Wiener was able to predict the actions of an aircraft pilot with sufficient accuracy that the guns could fire at the point the aircraft would be when the bullets reached it. Wiener's breakthrough was that it wasn't important to know, in advance, anything about the pilot or aircraft; rather, by observing their actions and movements, and analysing patterns within these, enough information could be gathered to make the necessary, precise prediction of what would happen next. In this sense, pilot and machine were taken together as an unknowable 'Black Box', as a model simplified enough to describe it to the rudimentary machines of the time. After the war, Wiener would take this principle forward, becoming a founder of the discipline of 'Cybernetics'.

In his book 'An Introduction to Cybernetics', W. Ross Ashby discusses further the ideas of the Black Box, providing us with a bridge between its electrical-engineering origins and Wiener's appropriation for use on a wider range of more complex systems. Rather than using the Black Box as a tool to gain understanding through simplification, Ashby discusses it as a problem to be tackled. He presents the lack of understanding as problematic, something to

be overcome by the experimenter's use of "certain given resources for acting on it (e.g. prodding it, shining a light on it) and certain given resources for observing its behaviour (e.g. photographing it, recording its temperature)."[2] He gives the example, again military in its origin, of an engineer required to investigate a broken, but top secret, bomb sight:

> "Sometimes the problem arose literally, when a secret and sealed bomb-sight became defective and a decision had to be made, without opening the box, whether it was worth returning for repair or whether it should be scrapped."[3]

With a fundamental distrust of its users, the Black Box, here, becomes a strong manifestation of hierarchical control. The engineer is required to maintain a device, but not trusted to understand it fully, allowed a level of control over its destiny, perhaps, but not able to do this from a position of comprehension: the balance of power is maintained in favour of the Black Box.

For Ashby, the Black Box problem takes one of two forms: 'The Very Large Box' and the 'Incompletely Observable Box'. When Ashby was writing the miniaturisation of general computing devices that has occurred today had not begun, and increases in computational or technological complexity necessarily increased the size of the object housing them. Today, elaborate systems can still be found. Despite their small size, modern computing devices such as smartphones and laptops are highly intricate computers[4], the phrase Very Large Box, then, describes an incredibly complex system and will be used here in that sense. As for the Incompletely Observable Box, early computers were of considerable size, often taking up rooms, or sets of rooms, but it was possible to see their whole, even if it was necessary to climb inside them, and initially at least it was possible to understand their construction by looking at them. The phrase in this context refers to devices, such as the bomb-sight, which were made inaccessible by structures of control, by legislation and secrecy, and in this sense remains relevant to the discussion here, but it is also worth considering for another reason: the internet, the global network joining many computers and devices around the world has produced technology that cannot be easily seen, both because of geographical

2
W. Ross Ashby, *An Introduction to Cybernetics*. (London: Chapman & Hall Ltd, 1957) p.87

3
ibid.

4
As well as regular phones and tablet computers, thermostats, watches, vacuum cleaners, light bulbs, speakers, thermometers, microwaves, pacemakers, bike locks, signs, bins, washing machines and so on.

inaccessibility, with cables running along seabeds for example, and its scale, stretching around the earth and, through satellites, into space.

The Black Box does not spring into existence, fully formed, as a large, complex entity. It grows through an iterative process of exploration and solidification of knowledge, Bruno Latour discusses this in terms of the progression of scientific ideas and theories[5↘] and, in terms closer to the Black Boxes discussed here, Garnet Hertz, in 'Art After New Media', shows a technology's progression towards a "single punctualized object"[6↘] which is used, not understood and calls it "a requirement of infrastructure and technological development". These singular, "punctualized" objects are a large part of the tools and appliances we use day to day. Our usage and understanding of them is presented in terms of input and output and, as far as our comprehension goes, they are Black Boxes. With wide network capabilities, trade secrets and and laws preventing their full inspection[7↘8↘], they are Very Large and Incompletely Observable in the fullest sense of the terms

Before moving on to the core examples of the Black Box, it is important to note that, while this essay will discuss Black Boxes mainly in terms of computational technology, networks and devices they do, of course, occur elsewhere, offline. Equally, there are computational technologies that are not Black Boxes and they are often intentionally and vociferously transparent. One umbrella that such tools fall under is 'Free Software', a movement initiated by Richard Stallman upon announcing his intentions to create an alternative to the UNIX operating system that would be free from usage restrictions[9↘]. It is not possible, due to space restrictions to discuss this in depth here but, for completeness, a brief outline is necessary. Free Software provides its users with a number of freedoms, ranging from access to the source code of the programs they run to the freedom to modify and redistribute them, allowing them to move away from the control exercised by software[10↘]. The word 'free' refers not to monetary freeness, but liberty[11↘]. This freedom, however, is very localised and can, by its nature, only be exercised within an environment over which the user has complete control to install this software, freedom to modify it means that, while one's own copy may be privacy enhancing, a similar program elsewhere could be problematic. This is compounded by the fact that many of the devices users interact with in the course

5
Bruno Latour, Science in Action: How to Follow Scientists and Engineers Through Society. (Cambridge, Massachusets: Harvard University Press, 1987)

6
Garnet Hertz, *Art After New Media: Exploring Black Boxes, Tactics and Archaeologies* (Leonardo Electronic Almanac, Vol.17, No. 2) p.205

7
https://www.eff.org/issues/drm (accessed 2nd June 2014)

8
https://www.eff.org/issues/cfaa (accessed 2nd June 2014)

9
Richard Stallman. *new Unix implementation*. 27th September 1983. http://www.gnu.org/gnu/initial-announcement.html (Accessed 24th September 2014)

10
The Free Software Definition. http://www.gnu.org/philosophy/free-sw.html (Accessed 24th September 2014)

11
Free Software is sometimes, for this reason, referred to as Libre Software, or FLOSS (Free, Libre, Open Source Software).

of using computational technology are networked and, as we will see in the next section, they present this with varying degrees of legibility to their users, making it difficult to know exactly what is being used and making it impossible to ensure a fully free interaction.

1.1 ↓ Opaque Interfaces

Digital consumer devices and services do not always offer up legible presentations of what, exactly, they are doing. They offer interaction through graphical user interfaces (GUIs) designed to make it easy and quick for the user to achieve their aims, and the fields of Human Computer Interaction and User Interface/User Experience (UI/UX) Design have focused, in part, on these interfaces, using affordances and metaphors[12] to achieve smoother, more usable, software tools. This, however, often hides underlying processes and activities of the devices in use.

The Digital Personal Assistants found on many smartphones, such as Siri for Apple's iOS[13], or Google Now[14] for Android and iOS based systems, are services which allow you to "use your voice to send messages, schedule meetings, make phone calls and more"[15]. These pieces of software, as presented by their interfaces, listen to your voice commands and queries, responding to them by scheduling items in your calendar, setting alarms or writing emails. Beyond this, they are able to search for facts and nearby amenities. Here, Apple's original version of Siri, released on October 4th 2011[16], will be used to explore the ways that User Interfaces can obscure the actions of software.

Apple's initial release of Siri used speech bubbles, similar to those found in the iOS messages application (→ *fig. 1*), to present a conversational view of the user's interaction with Siri[17]. This, coupled with the fact that the assistant can act on programs within the phone, gives the impression that it inhabits the phone, that any processing or cognition occurs within the user's device. If this is the case, although the user may not understand the exact way in which it works - it is certainly a Black Box - they surely have access to all the inputs (voice requests, the information on the device) and outputs (organisational software, the screen, the speakers) necessary to conduct an investigation of the Black Box.

This is not the case. It is, in fact, a carefully constructed

12
Joel Spolsky, *User Interface Design for Programmers* (Berkley CA: Apress, 2001), p.23 -31

13
https://www.apple.com/uk/ios/siri/ (accessed 2nd June 2014)

14
http://www.google.co.uk/landing/now/ (accessed 2nd June 2014)

15
https://www.apple.com/uk/ios/siri/ (accessed 2nd June 2014)

16
http://www.apple.com/uk/pr/library/2011/10/04Apple-Launches-iPhone-4S-iOS-5-iCloud.html (accessed 10th August 2014)

17
Siri is the name of the piece of software, but is also used as a 'name' for the 'assistant' - the voice the user hears.

fabrication. The conversational metaphor, the presentation, and the pacing of the interaction, hide a necessary offloading of processing. The devices on which these assistants run are not powerful enough to undertake the complex analysis required for the illusion of human-machine conversation, they must send the audio to remote, high powered data centers for processing[18]. In this sense, the device and its personal assistant are really just a node in a larger network, passing information to, and receiving it from, remote servers sometimes known as the 'Cloud'.

While this is, perhaps, fine while virtual assistants are pleasant, seemingly neutral, servants of the most banal scheduling needs, with some entertaining gimmicks thrown in[19], what happens when they are relied on for more personal, private problems, perhaps relating to health? What does it mean for something understood as a personal service to be part of a large external network, and what happens when these tools reveal themselves as especially partisan gatekeepers of knowledge?

Upon launch, it was discovered by users that "Siri failed to locate nearby abortion clinics. In some cases it suggested pregnancy advice centres as an alternative"[20], providing a biased, or skewed, filtering of information. Further to this, around seven months after Siri's launch, asking it the question "What is the best smartphone ever?" provided a result from the third party computational search engine Wolfram Alpha[21] naming a recently released phone by rival company Nokia. A few days later it had ceased to do so, instead providing 'humorous' replies such as "Wait... there are other phones?"[22]. The unwillingness to locate abortion clinics was eventually rectified by Apple, who asserted that it was not intentional, but the same capability to increase the impartiality of the tool was used, later, to control access to information on rival devices.

When a change is observed in, or a problem found with a tool (or a multi faceted service, masquerading as a tool) such as this guidance can be taken from Ashby, the engineers, and cyberneticians: the next step is to interrogate the tool as a black box.

Firstly, the inputs need to be monitored. These are knowable, on the simplest level they're the queries the user speaks and, delving a bit deeper, the settings on the phone and the information in its address book, calendar and so on could be considered an input.

18
http://www.smartplanet.com/blog/smart-takes/say-command-how-speech-recognition-will-change-the-world/ (accessed 3rd June 2014)

19
http://shitthatsirisays.tumblr.com/ (accessed 3rd June 2014)

20
http://www.bbc.co.uk/news/technology-15982466 (accessed 3rd June 2014)

21
http://www.bbc.co.uk/news/technology-18071342 (accessed 10th August 2014)

22
ibid.

Fig. 1.
Side by side Siri and messages screenshots showing the similarity of the interface metaphors.

Siri

Messages

Then, the outputs from the system should be measured. These are the qualifying statements and questions the assistant uses to focus the human language it receives into machine readable queries, and the results the assistant returns from these.

Though the inputs are adjusted and the outputs are compared scientifically and systematically, it's still likely that the results will contain a strange bias. As a result, expanding the area of investigation can lead only to the realisation that this device cannot possibly contain so much information about such a range of topics, including those that are time and location sensitive, it must be querying information services elsewhere (such as the aforementioned Wolfram Alpha). It is, therefore, not just a Black Box but, rather, a Very Large Black Box. Leaving aside their own status as Black Boxes, the search engines and other sources the assistant queries can be questioned in the same way it does[23], but still different results will be received. For example, while Wolfram Alpha informs the user that the best phone to buy would be a Nokia, Siri is insistent.

The conclusion to be drawn, then, is that, despite being presented as a self contained, localised system, this piece of software is, in fact, a node in a distributed, networked system containing both publicly accessible services and inaccessible proprietary services - the hidden systems within Apple's data center. It is certainly a Black Box, but now revealed as an Incompletely Observable Black Box. Aspects of the service are intentionally hidden for two main reasons. Firstly, the purposes of user experience, allowing the user to feel they are able to query their device directly which gives an illusion of efficiency, sleekness and privacy. Secondly, for the purposes of business, both overtly, ensuring the presentation of only Apple's services, and covertly, hiding the systems involved, the algorithms and data behind such services being a valuable trade secret.

Although one of the examples given above is ostensibly playful and tongue in cheek, they both show that the power lies with the software as a gatekeeper of knowledge. While it is possible for the user to know how a piece of local software functions by observing it, much like a traditional electronic device, when much of the functionality is external it is possible, and almost guaranteed, that it will change, constantly shifting the power relationship between user and device.

23
This requires a fair amount of assumption - the nested levels of Black Box involved here start to bring in a fair amount of opacity

1.2 ↓ Leaky Connections

While seemingly local devices may hide their true, networked, nature behind user interfaces, what of the internet, the World Wide Web, surely there's no artifice there? It's part of a web browser's presentation, via the address bar, to show that a website is separate from the user, the content changes without their control and when there's no connection, there's no access. However, while the user may be aware of their connection to a network, it's not necessarily clear what, or how many, parts of that network they are connected to. It's normal to visit a web address (for example, http://www.bbc.co.uk/news/) which returns specific content and one might logically assume that signifies a connection only to the single place that content is held, in this case on the BBC's servers.

It is possible to test this assumption. Many modern web browsers, such as Google Chrome provide tools for web developers to profile the sites they are building, to check loading times and other aspects of their performance, and these tools can be used on any publicly accessible site. Visiting news.yahoo.com[24↘] and viewing the network connections made, it can be seen that, in total, there were 100 requests made in the 10 seconds it took the site to load. Of these, 57 were from domains identifiably related to Yahoo, such as ads.yahoo.com, or l.yimg.com, with the other 43 coming from other domains with variable levels of identifiability: googleads.g.doubleclick.net explains itself, to a certain extent, while something like s1.2mdn.net offers little in the way of clues[25↘]. This can be seen on many sites across the web, bringing in data related to advertising, page content, user tracking, page analytics and so on.

Some of these further requests came from the page initially loaded - for example adding the images that were part of the layout, or scripts to add functionality[26↘] - but others were loaded in by other scripts. For example, inspecting one resource from http://ams1.ib.adnxs.com shows that it is a piece of javascript which loads in a further piece of javascript from http://cdn.adnxs.com which itself loads content from, or sends data to http://ib.adnxs.com. Visiting the last URL provides nothing human readable, so it's logical to assume that it's providing information to a server.

Some browsers do provide an indication of the connections a site makes, often as a small tab in the bottom left of the window

24 http://news.yahoo.com was the most visited news site according to Alexa's top 500 sites list (http://www.alexa.com/topsites/category/Top/News) at the time of visiting (28th August 2014). Except for http://reddit.com, which I'm even more unsure about classing as a news site than I am Yahoo's.

25 2mdn.net is registered to Mark Monitor, a brandprotection provider and a part of Thomson Reuters. But visiting the page returns nothing.

26 HTML, the primary language used to markup and build websites, provides only structural and textual content within its files, further resources such as images or videos are stored as separate files on the same, or different servers and referenced from the HTML.

which displays the current resource being loaded, but this not often particularly visible and ordinarily operates in real time which, given the speed of networks (UK average, 17.8Mbits[27]), and the small size of the resources loaded means that it's unlikely that users will see all of them, or even necessarily perceive that there are any at all.

Coupled with the inability to see the processes occurring on external servers, beyond the URLs accessed and the files they return, the nebulous nature of visiting a web pages shows the internet to be an Incompletely Observable Black Box. It is possible to get a sense of the requests and actions undertaken by a web browser but, as with the third URL linked above, the investigation can be quickly brought to a halt by a further Black Box whose inputs can be seen, but whose outputs are hidden.

These outputs can, therefore, lead anywhere and it's very difficult, if not impossible to know where this might be, at least just by investigating the technology available to us. The documents released in early 2013 by NSA whistleblower Edward Snowden make it clear that it's often impossible to know what's being done with our digital information, the extent to which this data is collected, redirected, stored and analysed means we have little to no idea exactly what's occurring, when and to whom.

They do, however, go some way towards revealing some of what might be happening to our data. The documents reveal 'Optic Nerve', a program from the British agency Government Communication Headquarters (GCHQ), which collected images from the webcam feeds of Yahoo webcam users, storing them for analysis. In this case Yahoo, the provider of the service, "denied any prior knowledge of the program, accusing the agencies of 'a whole new level of violation of our users' privacy'"[28], but the problems are similar whether the service provider is aware, or not. Networks, especially the internet, necessarily require passing of information to multiple parties, if it is not possible to know what happens at each step, with each party, then it is not possible to know, with certainty, every resting place for the data sent, and what has been, or is being, done with it. By trusting conversations and images to a service that functions as a Black Box, users are, in turn, opening their data to a larger network of collection, sending it to unknowable numbers other Black Boxes. Optic Nerve is just the program that has been made public. It is not possible, without

27 http://stakeholders.ofcom.org.uk/market-data-research/other/telecoms-research/broadband-speeds/broadband-speeds-nov2013/ (accessed 29th August 2014)

28 http://www.theguardian.com/world/2014/feb/27/gchq-nsa-webcam-images-internet-yahoo (accessed 5th June 2014)

further leaks, to know what, or how many, other similar programs there may be.

1.3 ↓ Talkative Objects

Lacking a full understanding of the machinations behind an optional digital assistant on high-end smartphones, and having assets loaded into web pages behind the scenes could be seen as optional problems. After all, if one doesn't want to talk to a smartphone, search engines are still available, and if the internet seems too opaque then there are still libraries and information centers, at least for the time being. The problem is only one part, of some parts, of two specific devices: the smartphone and the personal computer.

However, as part of the trends towards wearable technology and an 'Internet of Things', the number of devices on this network is growing in number and in variety of forms. Things that are traditionally singular, isolated objects are increasingly becoming computationally able, sensor rich, networked devices. These devices, formerly mute and static, are becoming talkative objects, with access, often very close, to information about things such as health, finances, relationships and with access to the wider network, they gain the ability to broadcast this to interested parties.

In his talk 'The Coming War on General Computation' Cory Doctorow highlights the changing relationship we have with computers:

> "As a member of the Walkman generation, I have made peace with the fact that I will require a hearing aid long before I die, and of course, it won't be a hearing aid, it will be a computer I put in my body. So when I get into a car – a computer I put my body into - with my hearing aid - a computer I put inside my body - I want to know that these technologies are not designed to keep secrets from me, and to prevent me from terminating processes on them that work against my interests."[29↘]

These computational, wearable and drivable devices are not just computers in terms of having processors, and running code, they are also likely to be networked devices too. In their paper 'Security and Privacy in Implantable Medical Devices and Body Area Networks'[30↙]

29 https://github.com/jwise/28c3-doctorow/blob/master/transcript.md (accessed 4th June 2014)

Rushanan et al. describe medical devices with the capability for "wireless data transfer (or wireless medical telemetry) for monitoring and configuration without sacrificing patient mobility or requiring surgical procedures to physically access the devices", revealing that these devices are implanted in more than 25 million patients in the United States[31]. The paper goes on to describe the difficulties involved in analysing the security of these devices, with "proprietary protocols" making it difficult for traditional tools to develop methods appropriate for analysing them. That the devices are seen as a Black Box even by the security researchers attempting to improve them makes it incredibly difficult to imagine gaining the assurances of control and knowledge Doctorow wants, especially at the level of the end users of these devices.

It may be unusual to consider a pacemaker, an insulin pump, or a hearing aid as a networked device, but there will be moments in their use where it becomes clear that they are. When a doctor wirelessly looks up the pacemaker's activation data to check that it's working correctly, for example. There are other devices, however, that may never make clear their talkative nature either because they are built to hide it, or because they are formerly mute objects and have been retrofitted to become vocal.

Germany's Der Spiegel, one of the recipients of Snowden's leaked documents published a number of pages from what they termed "The NSA's Spy Catalog"[32], a series of specifications, use cases and datasheets for some of the intelligence service's surveillance equipment. As part of this, they reveal devices that can be implanted in computers, routers and other pieces of network infrastructure, or placed within the signal chain to allow access to the information within them. For example, the 'RAGEMASTER' (→ *fig. 2*) is a 6mm long piece of circuitry, whose operation is outlined in its datasheet as follows:

> "The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminated signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor,

30
Michael Rushanan et al., *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy - SoK Track. May, 2014. Accessed 29th August 2014. http://sharps.org/wp-content/uploads/RUSHANAN-SOK-IEEE-SP14.pdf

31
K. E. Hanna et al. I*nnovation and Invention in Medical Devices: Workshop Summary.* The National Academies Press, 2001, cited in Michael Rushanan et al., *Security and Privacy in Implantable Medical Devices and Body Area Networks*.

32
http://www.spiegel.de/international/world/a-941262.html 30th December 2013 (accessed 30th August 2014)

NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the target monitor." [33]

Essentially, this tool silently copies the video signal being sent to a computer screen, while still allowing the original signal through, and can be queried by an external device to allow the intercepted imagery to be seen on a display external to the system, room and, potentially, building it is installed in.

In his keynote 'Art As Evidence'[34] at transmediale 2014, Jacob Appelbaum, a security researcher and journalist, and one of the first people to gain access to the Snowden files, discusses some of these devices and their implications. He describes the act of 'interdiction' undertaken by the NSA calling it "the process whereby all of those objects previously mentioned, gain a little extra attribute". Using an example of a keyboard ordered online by a fellow developer on the TOR project[35] he outlines the way that interdiction is used to intercept the package and, potentially, augment it with these tools for listening and broadcasting. As he says, it is not necessarily possible to be sure that interdiction, or other interference has taken place, and I would argue that this continues even if the devices are opened up and inspected. It is mentioned many times in the catalogue pages that the devices are often made from off the shelf components to ensure they cannot be traced back to the NSA.

Intercepting but not interfering with existing communications and piggybacking on existing networks allow these surveillance Black Boxes to take advantage of existing Black Boxed layer within the technology they surveil. By trusting our data and communications to one or more sets of Black Boxes, we open it up to many more. As Appelbaum goes on to say "When the physical world and the internet come together, there are these convergence points in which everyday objects are actually weaponised and turned against us". ↵

33
ibid.

34
Jacob Appelbaum: *Art As Evidence.* Transmediale 2014 Keynote. http://www.youtube.com/watch?v=ndx0eox0Lkg (accessed 5th June 2014)

35
TOR is a distributed network that helps provide anonymity for its users. More about TOR can be found here https://www.torproject.org/

Fig. 2.
The RAGEMASTER datasheet.
Showing the device, and outlining
some of its specifications.

RAGEMASTER

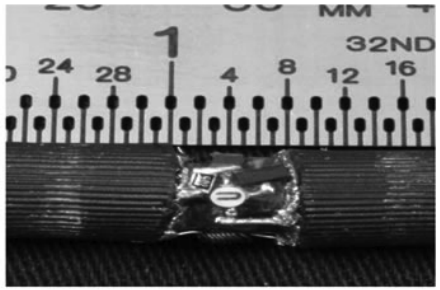
ANT Product Data

(TS//SI//REL TO USA,FVEY) RF retro-reflector that provides an enhanced radar cross-section for VAGRANT collection. It's concealed in a standard computer video graphics array (VGA) cable between the video card and video monitor. It's typically installed in the ferrite on the video cable.

24 Jul 2008

(U) Capabilities

(TS//SI//REL TO USA,FVEY) RAGEMASTER provides a target for RF flooding and allows for easier collection of the VAGRANT video signal. The current RAGEMASTER unit taps the red video line on the VGA cable. It was found that, empirically, this provides the best video return and cleanest readout of the monitor contents.



(U) Concept of Operation

(TS//SI//REL TO USA,FVEY) The RAGEMASTER taps the red video line between the video card within the desktop unit and the computer monitor, typically an LCD. When the RAGEMASTER is illuminated by a radar unit, the illuminating signal is modulated with the red video information. This information is re-radiated, where it is picked up at the radar, demodulated, and passed onto the processing unit, such as a LFS-2 and an external monitor, NIGHTWATCH, GOTHAM, or (in the future) VIEWPLATE. The processor recreates the horizontal and vertical sync of the targeted monitor, thus allowing TAO personnel to see what is displayed on the targeted monitor.

Unit Cost: $ 30

Status: Operational. Manufactured on an as-needed basis. Contact POC for availability information.

POC: [redacted], S32243, [redacted], [redacted]@nsa.ic.gov

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

2.x → STRATEGIC POWER AND TACTICAL RESISTANCE

2.0 ↓ Strategic Power

In order to begin to counter the Black Box, this weaponisation of everyday devices, it is necessary to come to some understanding of the source of its power. Examples of Black Boxes have been explored above, identifying their methods of secrecy and scale, and Appelbaum has offered a way, in the convergence points of the physical world and digital networks, to begin to identify them. Developing this, the Black Box can be seen in terms of the Strategy, outlined by Michel de Certeau in 'The Practice of Everyday Life', the technique whereby the powerful can "manage" the Other, and gain "mastery". Specifically, he defines it like so:

> "I call a *strategy* the calculation (or manipulation) of power relationships that becomes possible as soon as a subject with will and power (a business, an army, a city, a scientific institution) can be isolated … as the base from which relations with an *exteriority* composed of targets or threats (customers or competitors, enemies, the country surrounding the city, objectives and objects of research, etc.) can be managed."[36↘]

The Strategy "was military before it became 'scientific'" [37↘],

36
Michel De Certeau, *The Practice of Everyday Life* (Los Angeles, CA: University of California Press, 1984), p.34-39

37
ibid.

sharing an origin with the Black Box and allowing them to combine particularly effectively. The Black Box can be seen as affording the isolation mentioned by De Certeau as a prerequisite for the calculation and manipulation of Strategy, the exteriority, or targets, in this case are the users of the devices and systems. The Black Box is, therefore, granted the following three effects and advantages offered by the Strategy:

Firstly, in effecting the "triumph of place over time"[38] the place which a "subject" is able to delimit for itself allows it to "capitalize acquired advantages, to prepare future expansions" [39]. The Strategy, for De Certeau is very much spatial and this can be seen in the Black Box's capability for information collection, harvesting, for example, data the user inputs through a Graphical User Interface over time, in one place. Collating the occasional, temporal, interactions the user has with the device to a store of information such as a database is the Strategy's "combinatory organization of the movements specific to units" [40], a way of storing the actions of the user, readying them en masse for measurement, and analysis.

Secondly, Strategies allow the "mastery of places through sight" [41], they have the advantage, given by their establishment of place, of being able to "predict, to run ahead of time by reading a space" [42]. Many of the advantages of the example Black Boxes relate to this sight. For example, many of the external assets and scripts loaded in by web pages are used to observe and track users, either looking at their behaviour within the page, or their interests across the web for the purposes of targeted advertising, and the interdicted surveillance devices clearly make use of this sight. For this, the Black Box identifies its users, employing its Strategic "eye" to "transform foreign forces into objects that can be observed and measured"[43], its aim is the quantification of previous and current actions in order to predict and shape the future moves of its users. The Very Large Black Box in particular capitalises on its infrastructural, spatial gains, using them to envelop users within its boundaries, ensuring that every use of its gained space is clear within its view.

Taken together, the advantages the spatial triumph give the Black Box to collect and store information, coupled with the increasing ability, through "sight", to identify, observe and measure users, provide a platform on which it can build a store of knowledge. The

38 → 43
ibid.

collection of an unprecedented amount of information pertaining to the activities of its users allows the third effect of Strategy, the "power of knowledge"[44]. This collection and analysis of information is often discussed under the term "Big Data", referring to the increase in scale of data collection and analysis made possible by information technologies. Much has been written about its possibilities, including the suggestion that its scale would make possible the "End of Theory" [45], a powerful re-working of existing modes of knowledge that would *require* the Strategic benefits of the Black Box. If effected, a reframing of knowledge in this way, replacing the current use of scientific models which Anderson sees as "crude approximations of the truth"[46], with a new, algorithmically uncovered 'truth' through the mining of massive data resources, the creation of knowledge would only be possible for the Black Box. An ability to "throw the numbers into the biggest computing clusters the world has ever seen and let statistical algorithms find patterns where science cannot"[47], requires the availability of place, in order to create these computing clusters, for example; mastery over time, in order to run the statistical analysis; and the collection abilities given by its sight, in order to obtain a large enough collection of data points to allow the algorithms to pull out significant patterns. It is these patterns, inaccessible to those without these foundational powers, which allow the Black Box not merely to observe, but to come into possession of the knowledge necessary to begin to act and exert control over the behaviours of those external to it.

44 *ibid.*

45 Chris Anderson. *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete.* http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory (Accessed 11th September 2014)

46 *ibid.*

47 *ibid.*

2.1 ↓ Tactical Resistance

In defining the Strategy De Certeau is "concerned with battles or games between the strong and the weak, and with the "actions" which remain possible for the latter"[48], these actions are Tactics, and are initially described in terms of their deficiencies:

> "lacking its own place, lacking a view of the whole, limited by the blindness (which may lead to perspicacity) resulting from combat at close quarters, limited by the possibilities of the moment, a tactic is determined by the *absence of power*"[49]

48 Michel De Certeau, *The Practice of Everyday Life* (Los Angeles, CA: University of California Press, 1984), p.34 -39

49 *ibid.*

In outlining what first appear to be shortcomings, De Certeau firmly ascribes the Tactic to the weak, those who are unable to gain and make use of the advantages the Strategy enjoys, he refers to them as "consumers" and, notably in view of this discussion of computational systems, tools and interfaces, as "users". They are not beaten, however, by this lack of power: the Tactic provides and creates opportunities for the user. The "blindness" can lead to "perspicacity", making the user insightful, a very different type of vision to the wide view of the Strategy; the Tactic is urgent and, therefore, focussed. Appropriately for actions "determined by the absence of a proper locus"[50], a Tactic does not enjoy the same fixed form of definition as the Strategy, rather De Certeau describes it in fluid, fast terms as relying on "a clever *utilization of time*, of the opportunities it presents and also of the play that it introduces into the foundations of power"[51].

In terms of countering the all encompassing power of the Black Box, the Tactic is useful in that it doesn't require the user to escape the space in order to act, it presupposes that "it must play on and with a terrain imposed on it"[52] and therefore looks to ways to gain an advantage from within this internal landscape of control. With this acknowledgement, it becomes possible to imagine ways to counter the fixity of the Graphical User Interface, the endless collection undertaken in the name of big data, and the invisible watchfulness of the surveillance objects from within their structured, analytical, panoptic territories.

50 *ibid.*

51 *ibid.*

52 *ibid.*

53 David Garcia and Geert Lovink. *The ABC of Tactical Media*. http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html 1997 (Accessed 7th September 2014)

2.2 ↓ Tactical Media

In 'The ABC of Tactical Media' David Garcia and Geert Lovink use the "tactical/strategic dichotomy" from 'The Practice of Everyday Life' to "name a class of producers who seem uniquely aware of the value of these temporary reversals in the flow of power." and who "make the creation of spaces, channels and platforms for these reversals central to their practice"[53], they call this work "Tactical Media". These producers, then, are media manipulators, using, reusing and re-contextualising the tools of production to counter the messages of power. They need an awareness of the structure of media in order to begin this undertaking and this, coupled with the suggestion from Garcia and Lovink that they are "uniquely aware",

would seem to place them apart from the everyday that De Certeau outlines as a requirement for Tactics to maintain their advantages. Tactical Media does not sit well as an imposed, specialist practice and this phrasing has more to do with the nature of media in the early 1990s. The first 'Next 5 Minutes' Tactical Media conference was held in 1993, the same year the World Wide Web was released for free usage, therefore digital access to information was on a much smaller scale, with Tactical Media spreading through newsgroups and physical contact which would have necessarily given it a smaller reach than communication via the web.

Indeed, in 'Tactical Media', Rita Raley explicitly defines Tactical Media as being separate from imposed practices, contrasting it with the "California Ideology 2.0, whereby digital artisans articulate a vision of individual freedom realizable from within the structures of the network society"[54] and what she terms an Avant-Garde 2.0, drawing from Critical Art Ensemble, "whereby a technocratic class of resistors acts on behalf of 'the people'"[55], both of which are presented as a form of resistance implemented from above. These should be seen as an attempt to use the tools of Strategy for resistance, requiring a group, or class, to be fixed in place and remaining within the network structures, Raley's disparaging descriptions here outlining how they begin to turn intentions towards the maintenance of the structures they attempt to resist but, ultimately, rely on.

In the use of Tactics, through Tactical Media, the user is able to generate resistance without the need of the Strategic benefits of place and fixity. Freed from the need to stockpile power before being able to act, they become able to use the tools and structures of media to counter its messages. They don't, as Garcia and Lovink say, "just report events", they are "never impartial, they always participate"[56]. They cannot help but participate - they must act from within the structures they find themselves, from within the mainstream media landscape, and this makes them particularly accomplished at questioning and intervening in large scale systems using the "cheap 'do it yourself'"[57] tools that become available to them. For example, Raley's wide ranging exposition covers projects tackling issues such as border rights and immigration, military and recruitment propaganda, and the nature of financial markets, showing Tactical Media's fairly expansive vision, at least when taken as a field.

54
Rita Raley. *Tactical Media*. (Minneapolis MN: University of Minnesota Press, 2009) p.10

55
Critical Art Ensemble, *'Electronic Civil Disobedience'*, 1996, quoted in Rita Raley, Tactical Media, (Minneapolis MN: University of Minnesota Press, 2009) p.10

56
David Garcia and Geert Lovink. *The ABC of Tactical Media*. http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html 1997 (Accessed 7th September 2014)

57
ibid.

In terms of the Strategy/Tactic dichotomy outlined by De Certeau, the Tactic's identified advantages over the Strategy make it, and by extension Tactical Media, an effective manner of resistance against the Strategic aspects of the Black Box. ↩

3.x → OBFUSCATION AND MANIFESTATION

3.0 ↓ Obfuscation

The Black Box is, however, not merely Strategic, it has further capabilities, uniquely able to lessen Tactical Media's efficacy. To the three Strategic advantages the Black Box enjoys, I would add a fourth, consolidating and building on those provided to it by Strategy: *obfuscation*. The Very Large and Incompletely Observable nature of these networked Black Boxes means that many of their actions are illegible to those they seek power over; they enjoy the advantage of controlling the view others are able to have of them by only revealing the effects of their actions, that is, they are able to conceal much of the *place* they have reserved for themselves, ensuring that the form of expansive, searching *sight* they enjoy is unable to be used by adversaries to observe their workings. This not only allows them to hide the extent of their *knowledge*, but also prevents those in exteriority from gaining a similar level of comprehensive understanding. While the Black Box can see, store and analyse all that is external to it, the comprehension of the other is reduced through its lack of full sight and this further cements the *place* of control and power, allowing them to define what is "proper", a key part, for De Certeau, of their delineation of space in the first place.

In looking at the Black Boxes above, we saw that the inner

workings of algorithms are often closely guarded trade secrets. Gillespie, who discusses this, also analyses the role algorithms play as gatekeepers of knowledge, and the Black Box utilises these to cement its position as a gatekeeper of knowledge, able to conceal or reveal as much as required for the purposes of control:

> "Insight into the workings of information algorithms is a form of power: vital to participating in public discourse, essential to achieving visibility online, constitutive of credibility and the opportunities that follow. As mentioned before, the criteria and code of algorithms are generally obscured -- but not equally or from everyone." [58]

This obfuscation is not static though, as Gillespie says, algorithms are not equally obscured from all. Similarly for the Black Box's other tools: it is able to selectively reveal and conceal parts of itself at will, hiding its true nature and, to some extent, hiding its obfuscatory capabilities too. For example, a Black Box social networking service, such as Twitter, may allow users and developers to build tools on top of its systems or data. These might provide others with access to its content, or reorganise its content for a different purpose. This does not mean that they offer up the full service to the developers, but often they provide mediated access through an Application Programming Interface[59] (API), allowing a controlled level of interaction, for example, limiting the number of requests per hour. Although it may seem to be an open act, offering up some of the advantages it enjoys, the power remains firmly with the Black Box. Firstly, the process increases its reach - users have many ways to access it, and many views on it - and this increases its pool of available data and, secondly, the lifting of the veil is selective, revealing the tools to an observable, measurable set of users, and is by no means a guaranteed thing, the terms can be re-negotiated, the data made available can be changed or, indeed, the service can be withdrawn altogether.[60]

This changeability is not strictly within the remit of the Strategy, which plays the long game that access to spatial benefits affords it. In this sense, the Black Box is adapting to the advantages gained by Tactics, through Tactical Media, and in some respects is, itself, acting

58
Tarleton Gillespie *'The Relevance of Algorithms'* in *Media Technologies: Essays on Communication, Materiality and Society*, edited by Gillespie et Al. (Cambridge, MA: The MIT Press, 2014)

59
For a quick introduction to Application Programming Interfaces in an artistic context, see Jer Thorp's 'Art and the API' http://blog.blprnt.com/blog/blprnt/art-and-the-api (accessed 12th September 2014)

60
This was Twitter's progress. Gradually removing the access to its APIs that made it a useful, powerful tool for art, design and social analysis in favour of locking down its reserves of data and ensuring that the only entry point could be its own applications and website. See: https://blog.twitter.com/2012/changes-coming-to-twitter-api (accessed 12th September 2014)

Tactically.[61] It is able to use time to its advantage, and to operate in the realm of the tools that Tactical practitioners make use of, the cheap, easily accessible techniques of consumer technology. Through obfuscation, the Black Box has been able to infiltrate the tools of Tactical Media as they've matured, utilising the layers of complexity, the abstractions of the user interface, and the spatial fragmentation inherent to the server-network-node models of many connected tools to hide its capabilities, offering appealing alternatives or additions to these tools while cloaking their true capabilities for surveillance and control.

Obfuscation counters the Tactic in a further way, too, the Tactic must "vigilantly make use of the cracks that particular conjunctions open in the surveillance of the proprietary powers",[62] but the access to only the anterior, Strategically provided, obfuscatory elements of the Black Box, the user interface, the nodes at the edge of the networks, occludes these cracks, making them harder, if not impossible to find by chance in the solid surfaces of the Black Box. How can the user counter the power of the Black Box if it turns their tools, their Tactics, against them? How can they use the "tricks" if they cannot find the "cracks"?

It is not necessary to leave Tactical Media behind entirely in order to counter the mixed Strategies and Tactics of the Black Box, it continues to provide a wealth of opportunities and methods, rather it is important to turn parts of its attention to different places. To tackle its shortcomings it is necessary to act against and analyse the technological tools and methods of unquestioning use of these that allow the obfuscated Black Box to infiltrate the everyday practice and exert control.

3.1 ↓ Critical Engineering

Critical Engineering begins to offer us a way towards this, outlined in the 'Critical Engineering Manifesto'[63] by Julian Oliver, Gordan Savičić and Danja Vasiliev in 2011, Critical Engineering is a methodology for analysing technology and countering its control. It "considers Engineering to be the most transformative language of our time, shaping the way we move, communicate and think" while recognising that "each work of engineering engineers its user". This engineering of the user, the Tactical Media Practitioner, is part of the Black Box,

61
Potentially, this has become possible through Tactical Media becoming a coherent field via theorisation. Peter Lamborn Wilson's *Response to the Tactical Media Manifesto: A Network of Castles* contains thoughts on the problems caused by theory cleaning up the "filth" of Tactical Media, and some ways it can avoid them. http://subsol.c3.hu/subsol_2/contributors2/plwilsontext.html (Accessed 7th September 2014)

62
Michel De Certeau, *The Practice of Everyday Life* (Los Angeles, CA: University of California Press, 1984), p.37

63
Julian Oliver, Gordan Savičić, Danja Vasiliev, T*he Critical Engineering Manifesto,* 2011. http://criticalengineering.org/ (accessed 1st June 2014)

enabled by creating and acting upon, or rather *engineering*, tools.

There are crossovers and similarities between Tactical Media and Critical Engineering; for example, point 7 of the manifesto:

> "The Critical Engineer observes the space between the production and consumption of technology. Acting rapidly to changes in this space, the Critical Engineer serves to expose moments of imbalance and deception."[64]

This is Tactical action: acting rapidly, taking advantages of gaps that arise, exposure in moments of imbalance are where Tactics make their gains over the Strategy. Here, however, we see the area at which Critical Engineers are specifically aiming their critique: technology. In placing themselves between the production and consumption of technology, they begin to reject the unquestioning use of technological tools in some Tactical Media, but, by continuing to act Tactically, rapidly, and reactively, they stay away from the traps of the top-down digital impositions that Raley warns of.

'Newstweek',[65], by Oliver and Vasiliev, acts in this space before consumption. A device (→ *fig. 2*) that sits between the user of a web browser and the servers they seek to access, to read the news, it allows "citizens to have their turn to manipulate the press"[66], by intercepting the sites the users attempt to load and inserting information into them, for example by editing news headlines. While the device comments on the manipulability of the news and the media, it also makes salient points about the fallibility and potential bias of the methods we use to access and disseminate information. Highlighting the number of potential, often hidden, steps involved through displaying an adjusted final article, for example; but, also, through giving users access to the tools to intervene in these networks. The accompanying text states that "with the increasing ubiquity of networks and their devices comes greater ignorance as to their function, offering a growing opportunity for manipulation",[67] and, as well as being fully functional, and capable of being installed in public places, the project is exhibited in a gallery context as an interactive piece that allows visitors to manipulate the news on a local network. This brings the visitor into both sides of that space, they can attempt to consume information, seeing how it's manipulated and

64
Actually the 8th point, but the manifesto is indexed from 0, mirroring to the way that many programming languages refer to the first item in an array (a list) as item 0.

65
http://newstweek.com/ (Accessed 14th September 2014)

66
ibid.

67
ibid.

changed, and they can also act on the information, in the grey area of the delivery network, intervening in a step they, potentially, had not considered before when consuming information, a step that was previously invisible.

Much of the work of the Critical Engineers produces temporary alternative spaces that reflect the structures of wider networked, technological media, making them not only visible, but usable and allowing the visitor to see some of the hidden aspects of the systems. This is important in bringing threats, and control, to light; in 'Beyond Fear' Bruce Schneier discusses wide ranging security issues, but often uses networked technology as an example of people's lack of awareness, and the dangers of this: "The average computer user has no idea about the relative risks of … doing any of the dozens of things he does everyday on the Internet"[68] Discussing the widespread societal awareness, or not, of threats he makes a distinction between visible and invisible threats:

> "Slices of life with immediate visual impact get magnified; those with no visual component, or that can't be immediately and viscerally comprehended, get downplayed." [69]

The obfuscation in place as part of the Black Box's Strategies plays a heavy role in lessening the comprehension of its systems of control and the function of Critical Engineering is to counteract this, visualising the actions and magnifying their effects. Newstweek's two pronged attack on obfuscation does not remove it at source, but displaces the conversation about it, moving a representation to a space where comprehension is possible. It is particularly powerful in that it not only serves to show the visitors both sides of the Box, but it also, potentially, opens up a dialogue over its walls, the user of the adjustment software and the user of the edited news site being linked through their interactions.

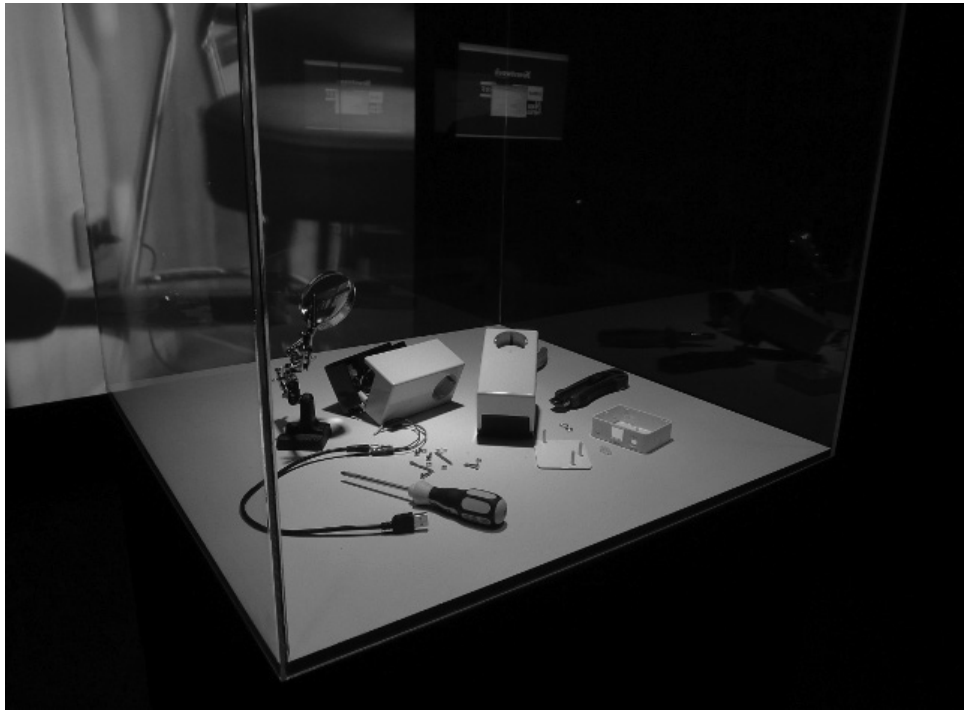
PRISM: The Beacon Frame[70], again by Oliver and Vasiliev, continues in the space between production and consumption, visualising hidden structures of control but it has a stronger emphasis on the tenth, and final, point of the Critical Engineering Manifesto:

68
Bruce Schneier. *Beyond Fear: Thinking Sensibly About Security in an Uncertain World.* (New York NY:Copernicus Books, 2003), p. 29

69
ibid.

70
http://criticalengineering.org/projects/prism-the-beacon-frame/ (Accessed 22nd September 2014)

Fig. 3.
Newstweek. A still from the video showing the device installed, and in exhibition, showing some of its components.



> "The Critical Engineer considers the exploit to be the most desirable form of exposure."[71]

An exploit, in computer science and engineering terms is a technique that makes use of a vulnerability in a piece of software or hardware to cause something unintended to happen.[72] Generally these involve running code on a remote system to gain access or information, for the Critical Engineer, though, the aim is "exposure", and as a result the "exploit" may not be the targeted, remote execution of malicious code on a computer system. In 'Beacon Frame', the system is the GSM mobile network, and it exploits the automatic connection of mobile phones to network towers. The piece, in its second form (→ *fig. 4*), consists of the "PRISM tower", which impersonates local cellular network towers, becoming a "rogue network" that nearby mobile phones will join automatically, "believing it to be trustworthy"[73] and a projection, a "rich and exploitative light show",[74] which shows information garnered from the phones that join the network; it also displays on nearby phones, sending those that join a message "of a troubling, humorous and/or sardonic nature"[75] The aim, however, does not lie here, although it operates within cellular networks, and exploits mobile phones, it aims for exposure of an invisible system. The project is a speculation on the form of the equipment the NSA use as part of their PRISM program, this is knowledge that, due to its secretive nature, is not publicly available; The project, therefore, raises awareness of the apparent ease with which a third party can insert themselves in the Black Box of the network. Offering speculation on how this might happen, and what it might look and act like is key to beginning a discussion on the issue, and to empowering citizens to gain greater understanding of and take action around the issues.

The intended exposure, then, took place with the project exhibited at Transmediale 2014 and the 'hijacking' of over 700 phones. Beyond this, however, a further level of exposure occurred: the piece was disabled. The accompanying site describes how, on receipt of a complaint, the technical contractor for the festival removed parts of the installation, preventing it from functioning, and threatened to call the police if it were restored. In a their response to this, the Oliver and Vasiliev quote Olof Mathe, the co-curator of the

71
Julian Oliver, Gordan Savičić, Danja Vasiliev, *The Critical Engineering Manifesto*, 2011. http://criticalengineering.org/ (accessed 1st June 2014)

72
http://blog.kaspersky.co.uk/exploit/ (accessed 22nd September 2014)

73
Julian Oliver, Gordan Savičić, Danja Vasiliev, *The Critical Engineering Manifesto*, 2011. http://criticalengineering.org/ (accessed 1st June 2014)

74
ibid.

75
http://criticalengineering.org/projects/prism-the-beacon-frame/ (Accessed 22nd September 2014)

event:

> "it's ironic that a component of the installation be taken down since it merely re-articulates some of the core questions raised by the piece: Who controls our infrastructure? Why is certain technology the prerogative of those in power? How can we foster public debate around the ramifications of technological choices?"[76↘]

In this way, although it was not intended and, perhaps, not ideal, the project in its disabled state continues to serve as a visualisation of some of the unknowable structures of control that the Black Box deploys and retains for itself: it remains to remind us that the interception of cellular networks by the Black Box is a legitimate part of the security apparatus, permitted for as long as it remains hidden and secret; the deployment of similar techniques in critically engaged artworks, in public ways that start debates and increase their legibility however, is actively discouraged.

Critical Engineering and Tactical Media come together in throwing the Black Box's smooth, seamless control into sharp relief. In making it, even in a temporary, rapid, Tactical way act against and highlight itself it is possible to counter the obfuscation employed by the Black Box, to begin to make the cracks that are necessary to open it further.

3.2 ↓ An Improved Apparatus

It is inherently difficult for the Tactical to make concrete gains against the Strategic, the lack of a place to stockpile its winnings and the reliance on opportunistic acts means that it is unlikely to build to a position of greater strength. As De Certeau says of the tactic: "what it wins it cannot keep".[77↘] This is not its aim, however, and, as shown by the disabling of 'PRISM: The Beacon Frame', the temporary nature can be beneficially leveraged. But only so much can be gained in this way, making the problem visible, asking questions and throwing the Black Box into the light. If the Tactic cannot stockpile its winnings, what can it do with them?

In his essay, 'The Author as Producer', Walter Benjamin calls for authors to be aware of the potential of their production in political

76
ibid.

77
Michel De Certeau, *The Practice of Everyday Life* (Los Angeles, CA: University of California Press, 1984), p.37

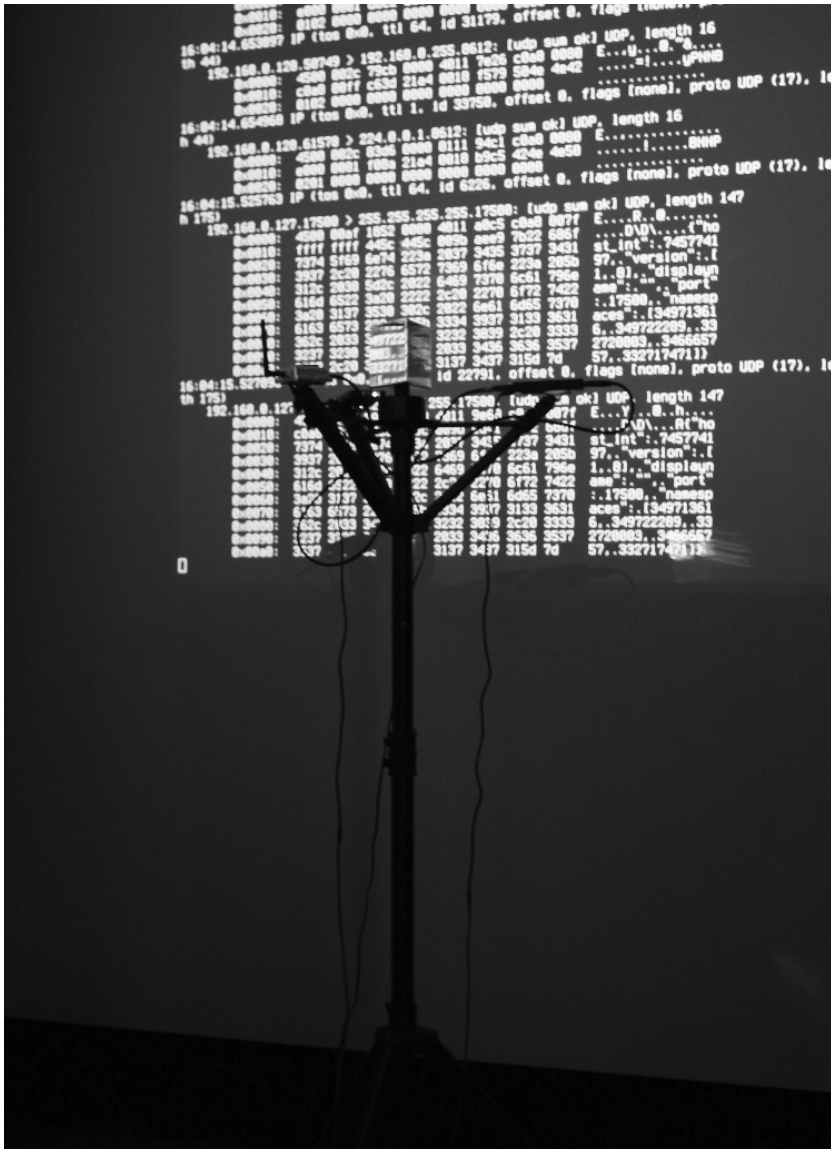


Fig. 4.
The “rich exploitative light show” of PRISM: The Beacon Frame.

terms:

> "What matters, therefore, is the exemplary character of production, which is able, first, to induce other producers to produce, and, second, to put an improved apparatus at their disposal. And this apparatus is better the more consumers it is able to turn into producers - that is, readers or spectators into collaborators."[78]

Benjamin traces the impact of authorial production from the initial act of creation, through its use as an improved apparatus, to its ability to enable consumers to become producers, or collaborators. Taken in this way, a Tactical act of authorship can be seen as having effects wider than its initial impact. Undertaken in a way that allow them to be utilised by others, these acts have the potential to become the improved apparatus, the producers of producers.

This process is part of the work of Critical Engineering, as outlined by its manifesto and the projects undertaken by its initiators. Some projects result in new tools, or instructions for their creation, such as Newstweek which, as well as being a device that allows its makers to critically engage with the distribution of online news, and which allows others to in a gallery environment, is accompanied by a web page detailing how to build a version of it, and a distribution of the necessary code and operating system to do so.[79] This serves two purposes. Firstly it places the message of the project in more than a single object, in a single situation; it allows it to exist in a wider way than if only Oliver and Vasiliev were able to easily produce the device. Secondly, it creates a platform, a stepping stone for others to look critically at issues stemming from or related to those highlighted by the project, it serves to create a potential open ended discussion around the manipulation of networked information, rather than locking it off as a fixed, didactic statement on the issue.

The Critical Engineers also offer a series of intensive workshops,[80] exploratory or instructive sessions which look at some of the issues raised by their work and, crucially, seek to impart their knowledge, their gains, to participants. From the description of their Networkshop:

78
Walter Benjamin, *The Author as Producer*, in *New Left Review*. no. 62, 1970. p83 - 96.

79
http://newstweek.com/howto (Accessed 24th September 2014)

80
http://criticalengineering.org/courses/ (Accessed 24th September 2014)

> "Learn how to create, analyse, manipulate and control computer networks using cables and the command line. Reveal network infrastructure by tracking packets across land and sea. Capture and dissect unencrypted data in the air around you. Assert your basic rights to privacy, anonymity and freedom of association using freely available, open-source tools."[81]

As part of the 5 day course participants are provided with a customised Linux operating system which contains network engineering and hacking tools, as well as instruction in how to use them, through the lens of constructing and manipulating computer networks. The practice of workshops in this way can be seen in terms of Benjamin's call, but pulling the three steps together; the work is authored and disseminated in the same space, tools are provided that are used cooperatively, necessarily leaning more towards the creation of collaborators over isolated producers and allowing for feedback loops to have some effect on the work produced. The nature of the workshops remains Tactical, they do not seek to attack the Black Box directly but, by highlighting and discussing issues through the practical application of computational tools, and the modelling of the structures of the Black Box, they are able to provide would be producers and collaborators with an awareness of its power and methods of control.

If Tactical Media is a resistance to the Black Box by the consumer, in the vein of De Certeau's everyday practices and Tactics, then Critical Engineering can be seen as building on this, implementing the exemplary production Benjamin writes of. It is not the genesis of this conversion of spectators to collaborators, rather Critical Engineering sits between the widespread re-appropriation of technologies by Tactical Media practitioners, as seen in the editing of technologies in Newstweek, and the broader culture of Free Software, as seen in the production and distribution of tools in the Networkshop, using the examples of both movements to inform its own production.

The tools provided by the Critical Engineers as part of their work and workshops are often existing pieces of Free Software, or built on top of them. For Benjamin, there is a key difference between the author as a "supplier of the productive apparatus" and the author

81 http://criticalengineering.org/courses/networkshop/ (Accessed 24th September 2014)

transformed into an “engineer who sees it as his task to adapt this apparatus to the purposes of the proletarian revolution”;[82] tools cannot merely be supplied, they must be improved and adapted for revolutionary purposes. For the resistance of the Black Box it is important to increase the legibility of its actions, this first and foremost means creating and distributing an apparatus that de-obfuscates its behaviour, this can be termed manifestation, a counter to obfuscation, allowing existing tools to make use of the cracks revealed, and this takes place in both the realm of public interventions and gallery-based installations, as well as instructional, collaborative spaces such as workshops. ↵

82
Walter Benjamin, The Author as Producer, in New Left Review. no. 62, 1970. p83 - 96.

4.0 → CONCLUSION

In the spirit of manifestation, this essay has aimed to draw attention to the Black Box, highlighting its edges, and delineating its processes and power. From its electrical engineering origins we have seen how it has solidified into a structure of power and control, capitalising on its Very Large and Incompletely Observable nature. The exemplary Black Boxes show the wide range of devices and networked tools that it resides in to do this, both overtly and escapably in consumer technologies, and covertly in the tools and techniques of global network surveillance, with cross pollination and collusion between the power structures of both.

The Strategic/Tactical dichotomy of de Certeau provides a useful way of understanding the power of the Black Box, as well as a beginnings of resistance in acting Tactically, however, as seen in the ways in which Tactical Media falls short in its face, the Black Box is able to cross such a rigid divide, able to implement Tactical actions to maintain its advantage. Its capability for obfuscation has been seen to confound the use and appropriation of consumer technologies, in which it hides, and require a further level of Tactical action.

In line with Benjamin's call for authors to recognise, embrace and expand the political nature of their work, providing an improved apparatus to allow consumers to become producers, Critical Engineering can be seen as a step forwards from Tactical Media, towards an improved apparatus for countering the Black Box. The creation of custom, enhanced tools is key here, as is a methodology for the dissemination of and education with them.

X ↓ Against The Black Box

The Black Box is powerful. It leverages its scale and complexity to gain advantage over its adversaries: us, its users and consumers. The black box is Strategic, first and foremost, consolidating its place, making use of its panoptic sight, and stockpiling knowledge; but it is able to build further on these advantages and act somewhat Tactically, flexibly obfuscating its reach and capabilities.

The Black Box is sleek and seductive, it gives us easy to use devices, tools and networks and, overtly, asks nothing in return. It exudes security, simplicity and seamlessness, promising to get out of the way and empower us. It offers this empowerment even for dissent, it swallows up social revolutions in its name, it offers tools which make it easier, faster, smoother to resist even the Black Box. It is difficult to avoid its charms, but the Black Box hides in these promises. It interdicts our tools and theories of dissent while allowing their delivery on and realisation via its structures and networks.

A new resistance is needed, and it must begin with knowledge, an awareness, first and foremost, of the Black Box, its locations and its methods. A Tactical knowledge to be spread and iterated on. This will be the necessary improved apparatus. Whether Tactical Media Artist, Critical Engineer or Author, in the face of an unknown and somewhat unknowable Black Box, manifestation, to reveal a segment, an action or some data from within or around the Black Box, is to strike a blow. Without its obfuscation it is merely another Strategic object, a large and complex one, perhaps, but susceptible to the same Tactical resistance as any other.

Bibliography

Anderson, Chris. *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*. Wired Magazine, online. 23rd June 2008. Accessed 11th September 2014. http://archive.wired.com/science/discoveries/magazine/16-07/pb_theory

Appelbaum, Jacob. *Art As Evidence.* Keynote Speech at Transmediale 2014. Berlin. Accessed 5th June 2014 http://www.youtube.com/watch?v=ndx0eox0Lkg

Ashby, W. Ross. *An Introduction to Cybernetics*. London: Chapman & Hall Ltd, 1957

Benjamin, Walter. "The Author as Producer" in *New Left Review* no. 62 (07, 1970) p83-96, http://search.proquest.com/docview/1036114365?accountid=28521

Bogost, Ian. *Alien Phenomenology or What It's Like to Be a Thing*. Minneapolis MN: University of Minnesota Press, 2012.

De Certeau, Michel. *The Practice of Everyday Life*, translated by Steven F. Rendall. Berkley and Los Angeles, CA: University of California Press, 1984.

Doctorow, Cory. *The Coming War on General Computation*. Lecture, Transcript. 28th Chaos Communication Congress. 27th December 2011. Accessed 4th June 2014. https://github.com/jwise/28c3-doctorow/blob/master/transcript.md

Foucault, Michel. *Power/Knowledge: selected interviews and other writings, 1972-1977*, edited by Colin Gordon. New York NY: Random House, 1980.

Garcia, David & Geert Lovink. *The ABC of Tactical Media*. 16th May 1997. Accessed 7th September 2014. http://www.nettime.org/Lists-Archives/nettime-l-9705/msg00096.html

Gillespie, Tarleton. "The Relevance of Algorithms", in *Media Technologies: Essays on Communication, Materiality and Society*, edited by Tarleton Gillespie, Pablo J. Boczkowski and Kirsten A. Foot. Cambridge, MA: The MIT Press, 2014

Hertz, Garnet, Art After New Media: Exploring Black Boxes, Tactics and Archaeologies in *Leonardo Electronic Almanac,* Vol.17, No. 2, 2012

Herzogenrath-Amelung, Heidi. "Ideology, Critique and Surveillance" in *Triple C: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* no. 11 (2, 2013), http://www.triple-c.at/index.php/tripleC/article/view/499 accessed 1 September 2014

Lamborn Wilson, Peter. *Response to the Tactical Media Manifesto: A Network of Castles*. 1st April 1997. Accessed 7th September 2014. http://subsol.c3.hu/subsol_2/contributors2/plwilsontext.html

Lanier, Jaron. *You Are Not a Gadget*. London: Penguin, 2011.

Manovich, Lev. *Software Takes Command*. London: Bloomsbury Academic, 2013.

Mazé, Ramia and Natasha Marie Llorens. "HOW does it happen and what does it take?", in *Design Act. Socially and Politically Engaged Design Today – Critical Roles and Emerging Tactics*, edited by Magnus Ericson and Ramia Mazé. Stockholm: Iaspis Konstnärsnämnden, 2011.

McEwen, Adrian and Hakim Cassimaly. *Designing the Internet of Things* Chichester: Wiley, 2014. Kindle.

Oliver, Julian, Gordan Savičić and Danja Vasiliev, *The Critical Engineering Manifesto*, 2011-2014. Accessed 1st June 2014 http://criticalengineering.org/

Raley, Rita. *Tactical Media.* Minneapolis MN: University of Minnesota Press, 2009.

Ratto, Matt. "Ethics of Seamless infrastructures: Resources and Future Directions." in *IRIE: International Review of Information Ethics* 8, 2007.

Rubin, Aviel D. *All Your Devices Can Be Hacked*. Lecture, Video File. TedxMidAtlantic, October 2011. Acessed 4th June 2014. http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked

Rushanan, Michael, Aviel D. Rubin, Denis Foo Kune, Colleen M. Swanson, *Security and Privacy in Implantable Medical Devices and Body Area Networks*, IEEE Symposium on Security and Privacy - SoK Track. May, 2014. Accessed 29th August 2014. http://sharps.org/wp-content/uploads/RUSHANAN-SOK-IEEE-SP14.pdf

Schneier, Bruce. *Beyond Fear: Thinking Sensibly About Security In An Uncertain World*. New York NY:Copernicus Books, 2003.

Sliwa, Jan. "Do We Need a Global Brain?" in *Triple C: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 11 (01, 2013), http://www.triple-c.at/index.php/tripleC/article/view/321 (accessed 2 September 2014)

Spolsky, Joel. *User Interface Design for Programmers* Berkley CA: Apress, 2001

Stallman, Richard. new Unix implementation. 27th September 1983. http://www.gnu.org/gnu/initial-announcement.html (Accessed 24th September 2014)