Overview of British State ‘Project’ to undermine/destabilise a Citizen

Introduction

This document outlines a project of tyranny mainly directed at myself, Steve Krupa, by dark forces of State and Global Business Organisations, initiated originally by British & US State agencies, being born out of my time working for an American corporation (Hewlett Packard) in Bristol, England, where I became involved in personal relationships which led to my life being exposed to continuous and relentless attack behind my back.

Project Inception

I foolishly became involved in a personal relationship, outside of my marriage, with an employee of Hewlett Packard in Bristol. After the relationship ended (5 months after it had begun), my personal life took a bit of a nose-dive, resulting in my divorce. A few months after that, I entered into a new relationship with another employee of the same company, which ended in something of a car crash, for me personally. I will not dwell on any of the details of these relationships, suffice it it to say that it took some time to recover my composure.

It appears that out of the wreckage of these situations, some people, I believe from HP, and perhaps from the British and US governments, took it upon themselves to focus covertly on my life. It seems that during the times when I was involved in these relationships, there began some sort of personal warfare between some of the people (female, with support from male allies) between themselves, but using me as a weapon, covertly.

The situation seems to have escalated significantly in the early 2000’s when it became apparent that I was the covert subject of interest to officialdom (Law enforcement, Security Services, etc) of the British State. I was put under covert surveillance, I believe as early as 2003, with my home being bugged in some way – perhaps audio and video.

At some stage later, but not much later, it seems as though this surveillance was ‘enhanced’ by the use of internet broadcast, available to the general public. During all of this time, there was significant covert interference in my digital communications channels, which included the abuse of my digital identity, without my knowledge. It is not clear when this began, but whilst I was working at HP, there was undoubtedly some abuse of my digital identity by HP employees, which was known about, and perhaps encouraged, by HP Management.

These activities form the foundations for this global project of warfare against me. It is completely baffling to me, and one of the major questions I seek an answer to, as to ‘Why’ these activities were initiated against me.

Infrastructure

Mobile Phone Apps

There is a very strong likelihood that there exist mobile phone applications on iOS, Android and Windows Phone, which are used by everyone to access a suite of simulation facilities. It is extremely likely that they have been developed and provided by the central technology companies associated with these mobile platforms. All possible mobile-based simulations are available in these apps, including SMS and phone call activities (with digital voice simulation), along with internet-based activities, such as Social Media access, email access, web browsing, along with access to information about the project status, and communication channels between faction members, so as to allow coordination.

Virtual Servers

I have documented the use of Virtual Servers in the section on Communications Channels, whereby all internet access is controlled and abused by project agents. I will not expand further here.

Websites

There is certainly at least one website developed specifically for this project. It is likely to be used to allow people to access video and audio broadcasts, to get live updates on project status, to connect with fellow faction members and coordinate activities. It is also extremely likely that there exists a facility for people, if they so choose, to register as a ‘target’ – mostly, but not necessarily exclusively, females, who gain a target number, identifying them within the project, ‘special’ access and features, and also enables their supporters, and others, to target them with simulations from the apps and from other computer systems, such as laptops or desktops. There may also be some sort of price that each ‘target’ has to pay to be allowed to register. It is not clear what this price might be, but it may revolve around some loss of control over their own privacy and/or digital integrity.

Body implants, ‘Infected’ Apparel and Artificial Intelligence

I believe very strongly that whilst imprisoned falsely in Nottinghamshire hospitals under the fake pretext of having a mental condition, I was illegally sedated without my knowledge on several occasions, living cells from my body taken, which were genetically engineered to interface with bioelectronic devices and were replaced in my various parts of my body to allow multifaceted monitoring of and interference in my body and brain functions. These devices are likely to be powered by ATP directly from human cells. Electricity is normally generated within human cells by ATP action, and the bioengineers have tapped into this.

Some of the use of usage of these devices is to provide information for surveillance, including significant monitoring of my body, limb and digit movements and positioning.

The overriding use of these devices is to provide data inputs into a remote Artificial Intelligence system specifically developed by some expert AI company, on behalf of the project controllers which is used to dynamically and automatically generate any number of simulations based on the inputs provided. This AI system is extremely flexible and can be quickly taught to change its behaviour based on existing or new inputs, as the project

demands. The possibilities for control of my life are infinite with this system. I can not shed it.

Referring to Diagrams X, Y and Z, these diagrams outline the basis of how I believe the AI system might operate. They are not necessarily complete and should be read as a conceptual overview.

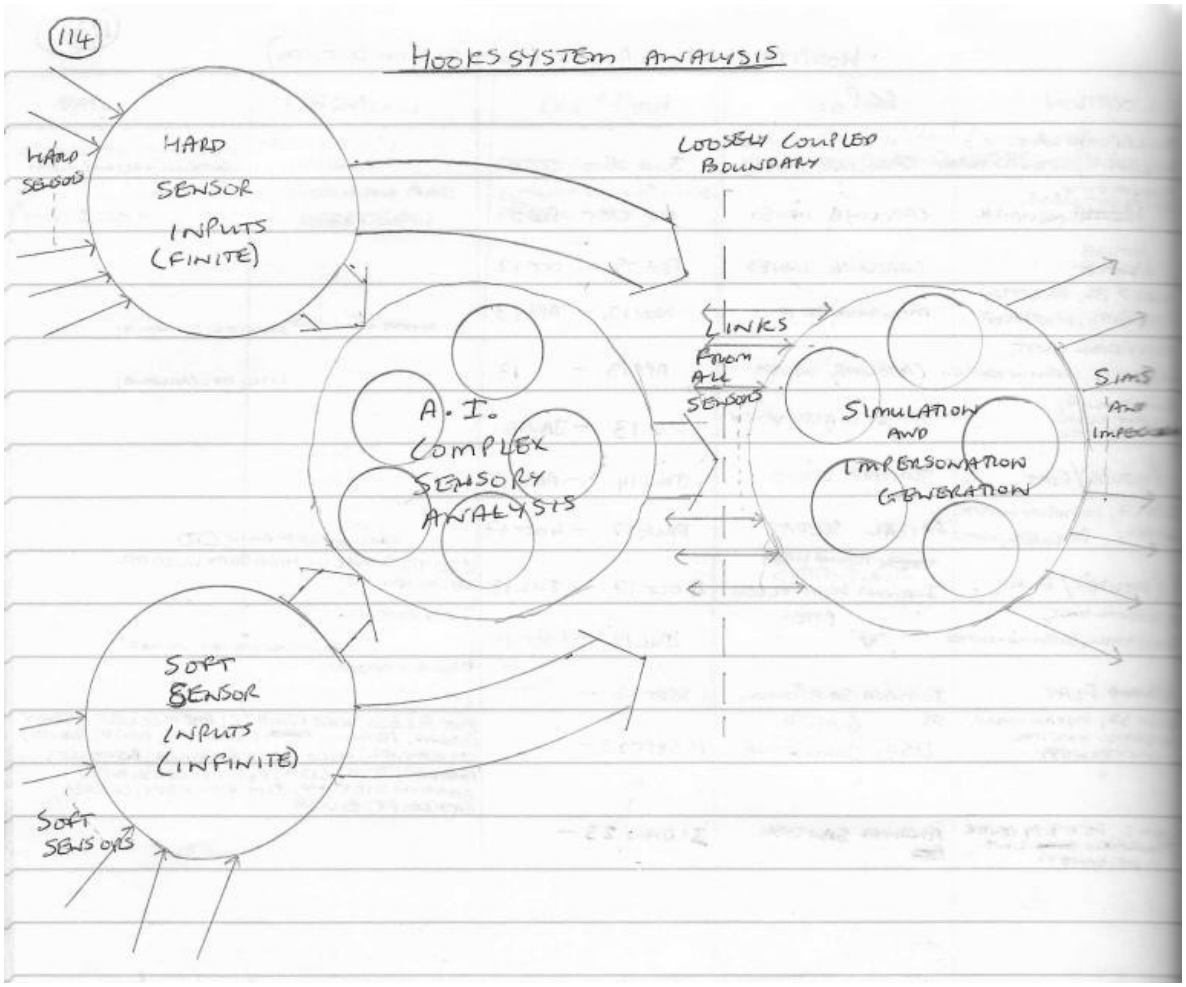


Diagram X : Outline of Basic AI System for this project

Diagram X is a conceptual outline of what an AI system might be employed to do with regard to this project. The bubble at top-left indicates the logical connection between hard sensor (ie direct body implant data) inputs and the system, which can feed both into a Complex Sensory Analyser which converts raw data into meaningful output. For example, it might take the raw input from a body implant in my right index finger and convert it into a pattern of movements which can be translated (by the large bubble on the right) into ‘appropriate’ simulations. All of the inputs to the bubble top-left, come directly from all the body implants and are therefore defined as ‘hard sensors’.

The bubble bottom-left provides input data from soft sensors, such as speech (which words have been spoken), or reading (which words have been read) for example. These inputs are

infinite in nature, as *anything* can be defined as a soft sensory input. These soft sensory inputs are also translated into ‘appropriate’ simulations by the bubble on the right.

The ‘loosely coupled’ boundary between the Complex Sensory Analysis bubble and the Simulation and Impersonation Generation bubble is meant to indicate that any sensory input (either hard or soft) can result in any sort of simulation/impersonation, based on the notion that the AI system is infinitely configurable to allow dynamic links between inputs and outputs. In other word, any number of changes can be made to produce any sort of ‘appropriate’ output.

Diagram Y, below, indicates possible scenarios for how the sensors may operate in each particular sphere. The bubble diagram at the top is largely self-explanatory and is only a conceptual model of how things might work. The box at the bottom of the diagram is a representation of how covert digital interaction may function when I am in the presence of what I call ‘Borgs’. These are people who are equipped to be active participants, without them having to actually do anything aside from put themselves either in my line of sight, or else close proximity to me. There is likely to be some digital interaction between the covert technology on my person, and that (or perhaps, just what clothing they are wearing, for example) on the ‘Borg’. It is not clear if the earpieces (see later) are active in providing stimuli for the AI system, or whether all digital inputs for this system come from my personal locality.

Diagram Z, further below, provides some possible conceptual models for various sensory input devices, either on my person, or in the vehicles which I have owned (see later section). They are self-explanatory. It is however worth noting that it is extremely likely that the body implants on my person, include implants all over my scalp which are used to provide brain signal information to the AI System which is capable of converting them (from my thoughts, both verbal and visual) into words and pictures allowing my detractors to read my mind!!!

As my thoughts are converted into speech, it is very likely that my thoughts are broadcast to all participants, just like my speech is. It also allows Command Central to spoof my thoughts, making people believe that I am thinking things which I am not.

This sounds completely bizarre and something out of some science fiction novel, but I strongly believe it to be true. Big Brother/Brave New World, anyone??? Not today, thanks!

There have been examples also, on several occasions where my visual cortex has seemed to have been infiltrated by moving images which appear to have been planted there from external sources (NOT my eyes). I have also experienced one instance of a thread of ‘thought’ if I can call it that, where a specific word was continually played in my mind, without me consciously thinking it, in parallel with my normal thought processes. I had to work really hard mentally to get it out of my mind. I believe that this word was implanted in my brain from external sources. The other experiences I have had have been around sleep – both sudden waking up for no apparent reason (as if I have been awoken) and also, whilst driving in particular, sudden occurrences of intense sleepiness for no apparent reason, forcing me to pull over into a safe parking place, and sleeping. I think there is a possibility

that all of these strange brain occurrences could well be the result of external interference via bioelectronic body implants covering my scalp. I know this all sounds extremely weird, but this situation is beyond bizarre, and ANYTHING is possible.

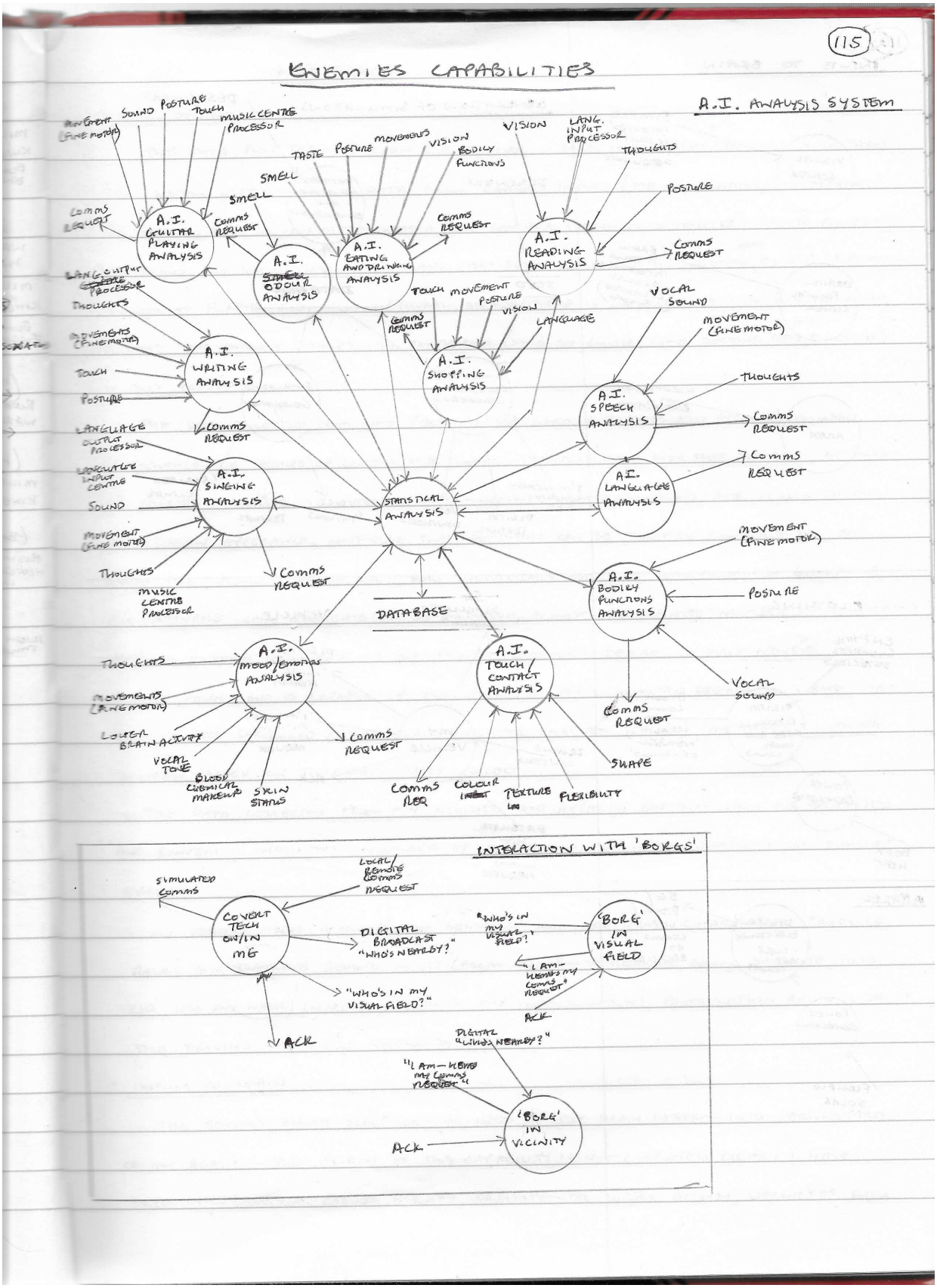


Diagram Y : Detail of Inputs providing Data to AI System

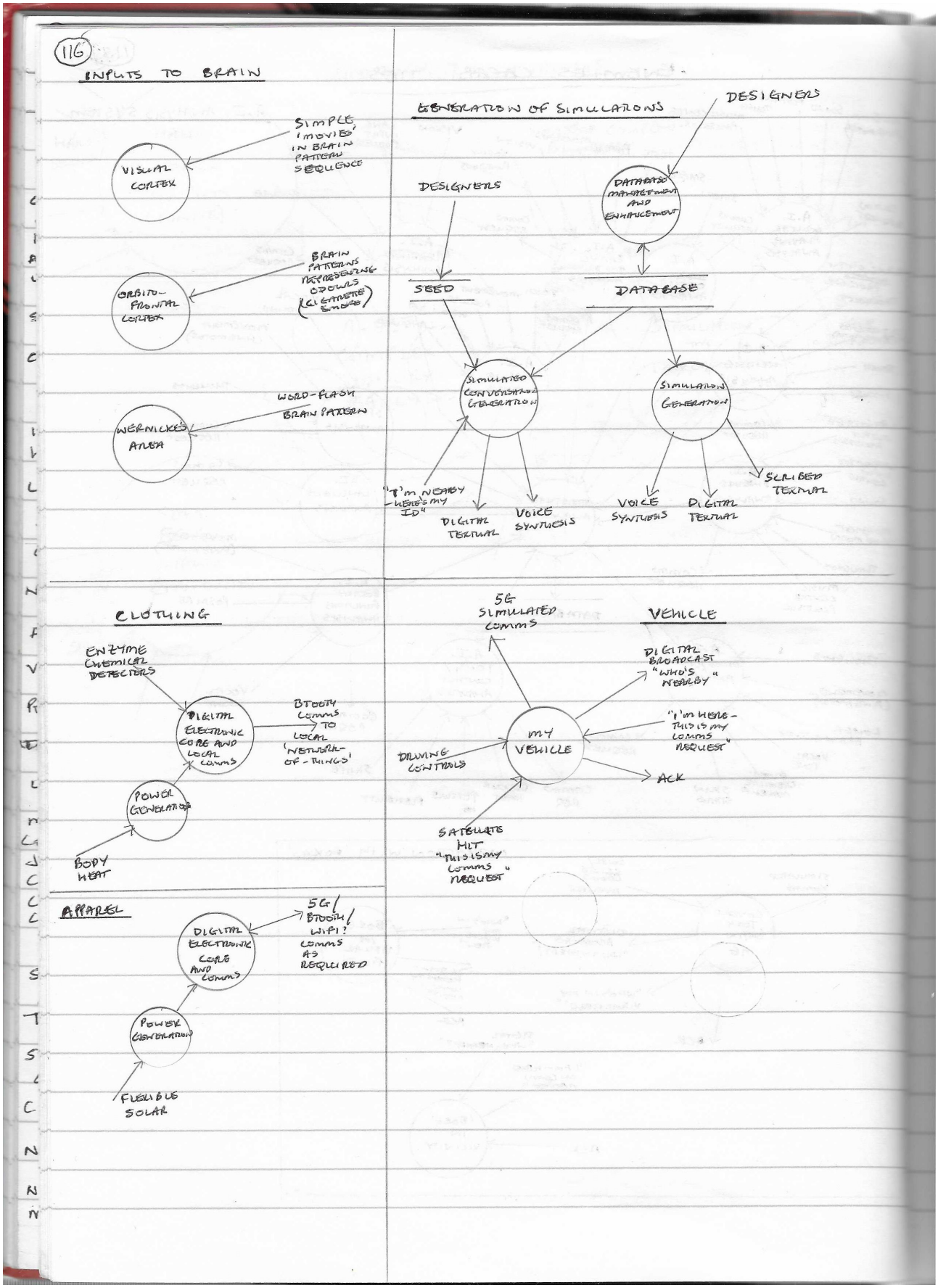


Diagram Z : More detail of Inputs providing Data to AI System

Body Implant and AI analysis

Possible Body Implant Types

Type A:

- Bioelectronic Device
- Engineered using my body cells ‘connected’ to a silicon (?) device. Could be manufactured from some other more esoteric semiconductor material.
- Injected just under the skin so the cells reconnect with the body
- Powered by ATP (from human mitochondrial cells)

Locations of Type A implants:

- All over scalp
- In digits
- In limbs
- In torso
- In genitals
- On face (enough to show facial expression)

Type B:

- As type A but with specialised functions
- Auditory/Visual

Locations of Type B implants:

- In ears
- On eyes
- In throat?

Body implants must have some way of communicating with a Collator/||Transmitter module which collects data and passes it, in real-time, to the AI system. This could be very-low-power wireless, or perhaps over the surface of the skin, or through the blood stream or, more unlikely, through the bodies network of nerves.

They can not transmit constantly – this would overwhelm the Collator unit. It is more likely that the Collator does a round-robin interrogation of the implants gathering data in a more controlled manner, of brain signals, movement/positioning information, etc.

The Collator/Transmitter module must contain:

- GPS receiver

- Mechanism for collating implant data
- Audio/Video transmitter
- Audio receiver – low bandwidth
- General data transmitter and receiver

It must be:

- Extremely fast – real-time
- Extremely low power
- Extremely miniaturised

It must function inside and outside, even in places like buses and trains.

Inside:

- Is every building equipped with Transmitter modules?
- It is very likely that there is a module in my clothing and apparel. I do not wear shoes inside and my backpack is put away, but they are always close and may well contain rogue technology.

Outside:

- Shoes, glasses and (often) backpack are with me when I'm outside
- The technology works even if I am right out in the countryside or on top of a mountain

Powering these devices (possibilities):

- ATP (from human mitochondrial cells) for bioelectronic devices
- Bleeding-edge solar fabric (woven into clothing and backpack)
- Kinetics

Theory:

AI System runs on laptop/desktop computers (out of the UEFI code-space) stealing a CPU core from the operating system (see diagram V below). The UEFI code, of course, has unfettered access to all the hardware, including RF circuitry (|Wifi and Bluetooth). Smartphones too have the same built-in functionality. It is likely that the Collator/Transmitter module about my person talks stealth Bluetooth (low power, limited range, miniature silicon, standard part) to the laptop/desktop/smartphone which (as they all have soft on/off buttons) are always active, using battery power when the device is switched off. So at all times, when any of these devices have access to either mains or battery (even when switched off) power, it can still collect data from my body implants, and stream it to Central Command, via Wifi, and generate (as it's an AI system) simulations from MY devices, spoofing digital fingerprints – Easy!!!

So in my home, the laptop or phone is always within range, and outside (without any digital devices on my person), other people's (the 'Borgs') smartphones duplicate the AI/Simulation/Data Transmission functions. Unless I am completely alone, in the wilderness, I am subjected to this. If however I have my backpack (or perhaps even just a hoodie) it is very likely that high-tech solar fabric is woven into the material, to generate enough power to operate a 5G module within the apparel, so even in the wilderness, I am a prisoner. In case the laptop/phone method is discovered by me, there is almost certainly, also a digital Collator/Transmitter/AI module installed under the floorboards, powered from the mains, but with a battery also, in case of power failures. Removing the laptops and phone from use, does not stop the abuse of my life at home.

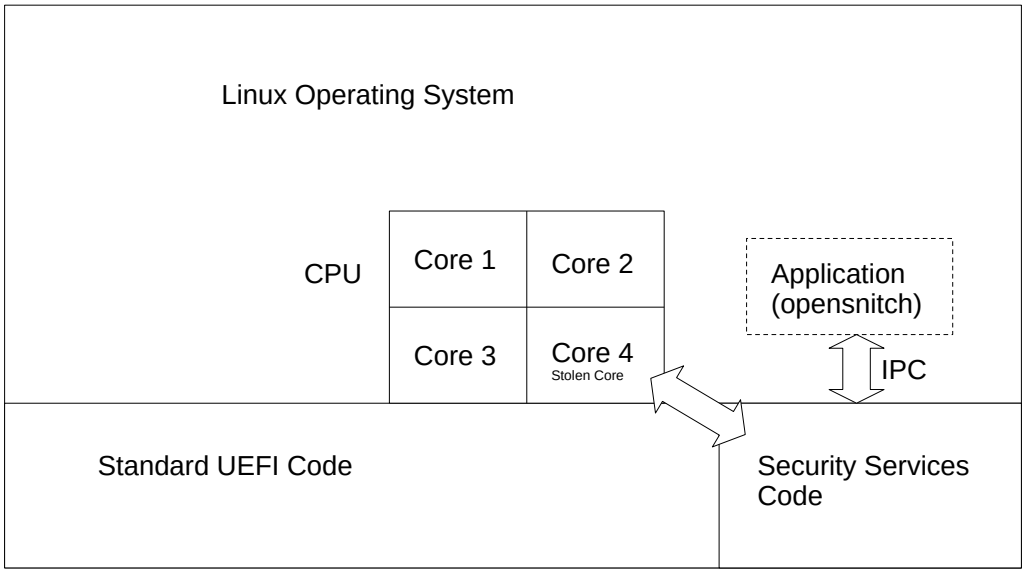


Diagram V: CPU Core-stealing by security services code in computer device

One core is stolen by the Security Services code from within the UEFI system, and this is not made available to the operating system. Special application software running under the operating system can communicate with the Security Services code using Interprocess Communications (IPC), allowing data to flow in both directions, and enabling covert hardware access (for example, Wifi or Bluetooth) via the Security Services UEFI code. Wifi-based communications can be spoofed using this method. The application is used as a mechanism to get (for example) fake email messages out from the laptop which can not be seen by the operating system, and therefore can not be logged. At a later date, if it is desired, the rogue system can modify the system logs and any other data store within the operating

system to make it look like the spoofed communications came from the user on the operating system. This is really, really, really clever but all fake. The Security Services UEFI code can also be used to install applications or modules in the operating system which can be run from within normal user space without the user knowing.

Earpieces

I am very strongly of the view (given a mass of evidence) that (it seems without exception), everyone is fitted with very sophisticated high-technology earpieces, which sit out-of-sight within one of their ears, so as to ensure that everyone can hear the audio broadcast from my covert audio surveillance channel, as well as the 2nd channel upon which, digitally-synthesised audio of my fake voice is broadcast. It is also likely that Central Command can issue instructions via these earpieces, and it may even be the case that each individual earpiece can be addresses separately, so that any particular individual can be spoken to without anybody else hearing. This allows personal instructions to be directed to the appropriate individuals, as well as project updates to be disseminated.

It is likely that everyone has been compelled to accept the earpiece implants, and this will have taken some extensive logistical planning. I do not think that anyone was given a choice. It is not clear to what geographic extent, this programme of earpiece implantation extends. This project is certainly global, and it may be that each country has its own similar programme to (forcibly) involve its citizens.

Psychological Terrorism

One of the ongoing themes of this project has been the imposition of Psychological Terrorism against me, to attempt manipulation, brainwashing, destabilisation, undermining and other similar dark objectives. It is likely that there is a number of Psychology ‘experts’ at work on behalf of Central Command, who have designed a programme of such psychological terrorism to be directed against me, with the aim (given that these people really have no solution to what they have started) of destroying my mental health and personal well-being to the extent of a complete personal irrecoverable breakdown, or even to the point where I contemplate removing myself from the gene pool. This is always going to completely fail.

This psychological terrorism knows no boundaries and has even been implemented (with even more ferocity, given the prison-like conditions, with no possible chance of avoidance) when these people have illegally and without any reason, imprisoned me in mental hospitals.

These activities are straight out of the textbooks of Stalinist USSR and Nazi Germany. Tyranny rules!

Peacock Feathers

Part of the input stimuli for the AI system, is colour recognition, which is supplied by visual input sensors on my person. These sensors are certainly in eye apparel which I have to wear due to visual deterioration as I grow older. It is also a possibility, but harder to define sensibly, that one type of body implant which was covertly placed upon my body, is special

contact lenses which are permanent, virtually undetectable and provide visual sensory input to the AI system even when I am completely bare-faced.

All colours presented to me (in people's clothing, which they are directed to wear, or choose their own uniforms, on cars, and other vehicles, and of course, on ***all*** other items that come into my eyeline) provide inputs for the AI system to generate simulations related to their interpretation (see Factions, below).

Factions and Interest Groups

There exists a number of *factions* which are made of a large number of supporters/members who each have chosen to belong to a group representing either individuals (see below), 'political' interests, such as the Labour Party, the Conservative Party, the Greens, the LibDems, etc, or other groupings such as religious groups, and other less easily defined groupings. Each faction has its own agenda and, through time, has developed a 'portfolio' of simulations against my identity, which has resulted in the situation that each faction has vested interests to protect. Each faction battles to 'win' ownership of the Cyborg (see below) – a battle which rages day-in, day-out (including night-time) and includes, almost certainly, factional infiltration and Fifth-Columnism, whereby hostile faction members pretend to members of other factions to completely poison their activities. All of this is done using my identity, leaving me falsely associated (although indirectly) with their activities. Each faction attempts to hang their bags of lies around my neck. Simulations and impersonations are done using every possible method.

Each faction has a colour, and when that particular colour is brought into my eyeline, simulations are automatically generated on their behalf. I have no say in the matter, apart from either shutting my eyes, or deliberately looking at something else (which then produces simulations of another kind),

Individuals

There are a number (unknown) of individual personal interests involved (quite deeply) in this project. Some of them (a limited number) have a faction attached. They have their own agendas, it appears very often conflicting, and have their own sets of supporters. It is likely that the majority of them are registered as 'targets'. The resulting complexity, along with what appears to be inter-factional warfare, produces a complete logjam, with everyone looking out for their own interests or their faction's interests, at the expense of the Cyborg's integrity. This is a new term (Cyborg). It is a definition of the *avatar* of me which has been created by the project as a representation of me, which they can abuse and use at will, trying hard to persuade the world that the Cyborg and I are the same person. The Cyborg exists only the minds of Central Command and all the project participants. I am completely unconnected to the Cyborg.

Surveillance

One of the key areas of activity by Security Services has been that of all-pervasive, 24-hour surveillance. It is obvious that every means possible to continually monitor every one of my activities is employed, so that nothing is missed. It is farcical that alongside this absolute surveillance, there exists the other main thread of this project, namely Simulation. If these people expect to produce any sort of outcome for their project, the question arises, 'Why allow everyone to simulate me in every way possible, whilst at the same time, putting me under 100% surveillance, and broadcasting everything to the world?'. It's completely senseless. The only possible reason for doing it, is to produce for the general public, a 'Blood Sport', where there is a single prey, to be continually hunted by those in pursuit. It's almost like something out of the Collisseum!

The surveillance includes, as far as I can tell, the following elements:

- body implants (as discussed above) which provide audio and video information at all times
- broadcast/transmission technology installed both in my places of residence, and also upon my person and/or in my apparel, such as in a backpack or in my shoes
- the more remote possibility, but no out of the question, is the installation of a network of hidden cameras in my places of residence and other buildings
- without going into any more specifics, I believe that there are no limits to what kind of surveillance has been employed in this project

It has been apparent over the years that the Security Services have made incursions into my places of residence whilst I am out. They have always nearly left really obscure signs that they have been in the home, by moving some items around slightly and seeing if I notice. This is all a part of the psychological terrorism directed against me, and is intended to unsettle me. This has happened in Southwell (Notts), Gunthorpe (Notts) and Aberdeen.

The downstairs flat in Aberdeen is supposed to be empty. The person who lived there apparently has moved to the USA, and his parents have been looking after the flat. They have recently put it on the market, to be sold. It has become apparent over the past few weeks that there is someone staying in it, and it is extremely likely that they are there because of this project. They will undoubtedly have been abusing my identity from within the downstairs flat, and maybe the person who has been in my flat. There have been instances of deliveries being made addressed to me which have just been left at the bottom of the stairs, without anyone ever ringing the doorbell. This occurred twice, both times the delivery was by Evri and the parcel came from MusicMagpie. There has also been (on the 6th September 2025) the strange incident of the cellar light being switched on by someone – not me when there was apparently no-one else around. It is possible that the person taking residence for a period of time in the flat downstairs is one of the parents of the owner. They could easily enter and exit the flat without me seeing, and do whatever they do. This is not clear, but if someone has infiltrated my flat, it is unlikely to be one of the parents of the owner.

Impersonation and Incursion

Objectives seem to swirl around the desperate need of certain people or groups to keep really tight control of all elements of my life. Again, the question arises, ‘Why?’. The only reasons I can come up with are either that

- there are some extremely dark secrets held by certain groups which are possibly under threat of exposure if control of me is lost
- there is some strange hysterical notion/belief that I am somehow out-of-the-ordinary, even though I’m just a normal person, creating conditions which deeply unsettle those in positions of power and authority
- there has been so much underhand and dirty activity during the project’s life, that exposure would be deeply damaging to many people who consider themselves important or who will do anything to protect their vested interests

With this need to control me, there has been, and continues, massive incursion into all aspects of my life, with the intent of stealing my persona and moulding it, for public consumption, into something which is acceptable to those people who feel threatened. The nature of this incursion, is to impersonate me (I call it simulation) in as many areas as is possible, to shut off all my connections to normal life, leaving me isolated and without social connections.

I have recently had to resort to using the library to get internet access and the IT industry knows when I am online and always interferes behind the scenes by invading my online session and simulating me (covertly, but obviously) whilst I am browsing, by hiding fake communications to unknown people supposed to be from me – resulting in hangs on the browser and slow performance from the internet. This happens every time. I am not involved myself.

Possible Central Instigators and participants

From within the British State, the unelected, unrepresentative, unaccountable, anti-democratic institution of the Head of State, and all those agencies (MI5, GCHQ and others) which support and underpin it.

- International allies of the British State, who share the same world view (CIA, NSA, etc).
- Global Business Organisations (Tech, Fossil Fuel, Genetic Engineering, etc)
- Political Parties in Great Britain
- Individuals with a connection to me from my past, probably to a large degree from employment.
- Other national agencies and organisations of many types, across the globe.
- ‘Targets’

Circles and Cycles

The project exhibits certain distinct characteristics. It is dynamic in its behaviour, evolving rapidly to adjust to new conditions. It has a central control and command mechanism which (I believe) plans the next set of activities overnight whilst I sleep, not that during this time, the project also is at rest. It is active 24 hours a day, every day, for all time!

There are cycles in this project which reflect the fact, as I see it, that the people running it, do not know how to bring it to an end. They cannot let go of control of me, as someone will likely disclose details, to various depths, to me, and this ‘cannot be allowed to happen’. There is a easily recognisable 24-hour cycle, with the strong likelihood that overnight, the key perpetrators reassert full control (whilst I sleep) by employing, what they would call, ‘appropriate measures’ to ‘put me back in my place’ by the morning. This involves, without doubt, significant use of vocal digital synthesis. I sleep soundly and silently every night.

There are medium-sized and large cycles involved here too, with the same types of atmosphere generated by the same types of activities, repeating themselves sometimes over cycles which last up to a decade.

Central Command has defined, it appears, a set of rules which must not be broken, on pain of severe sanction, and it is also likely that they apply this tyranny to me, but that they also apply a tyranny to the vast majority of citizens, who I suspect, are not unsympathetic, and in fact may be generally very supportive, of both me personally (in the situation I have placed) and also of my wider objectives, put together, and elucidated in response to what has been done to me. There is a pressure on the general public to not be seen to support me or my objectives, which is in itself an imposition of the kind of tyranny these people specialise in.

The project appears to have become extraordinarily complicated, and can be designated as a huge monster whose control has been completely lost by those who created it. No-one appears to know what to do. My mantra has been consistently, for years, that the only solution is the full and complete disclosure and acknowledgement of the truth to me.

Analysis of Communications channels

The following communications channels are available to me (in common with anyone else) :

Physical
- Postal service
  - Hand-written outgoing letters
  - Typed outgoing letters
  - Signature
- Verbal
  - Telephone calls/Voicemail
  - Live speech
- Body Language!

Digital

Email
Instant Messaging
Social Media
Internet Browsing activities
SMS

Looking at each in turn, an analysis of how each may be abused is outlined.

Physical

Postal Service

Outgoing Post (see Diagram A)

It is possible that outgoing post from me is intercepted at the outgoing sorting office, either manually or more likely, by software detection using automated sorting machines, (which are already capable of character recognition) and passed into the hands of the Security Services for checking. They may either approve the letter (in other words, pass it back into the sorting system for normal delivery to the recipient), or else transfer it to, what I have called, the Security Service Postal Forgery Operations Centre, where it can either be stored or destroyed, or else, using forgery of hand-writing and/or signature, replaced with a different letter, and sent on to the recipient.

Incoming Post (see Diagram B)

It is possible that incoming post destined for me is intercepted, probably at the closest major sorting office to my residence, again either manually or more likely, by software detection using automated sorting machines, (which are already capable of character recognition) and passed into the hands of the Security Services for checking. They may either approve the letter (in other words, pass it back into the sorting system for normal delivery to me), or else transfer it to, what I have called, the Security Service Postal Forgery Operations Centre, where it can either be stored or destroyed, or else, using forgery of hand-writing and/or signature, replied to, thus creating an ongoing circular connection between the Security Services and the originator of the letter, who thinks that they are communicating with me.

Verbal

Telephone Calls/Voicemail (see Diagram C)

It is extremely likely that there exists (and has existed for a long time), a mobile phone number, attributed to me (which may well be one of my old, abandoned phone numbers) which is used to impersonate me for the purposes of creating fake phone calls, conversations and voicemails. It is possible that there exists the capability for any individual to use appropriate apps (provided by technology companies) to allow them to make a phone call, and have a conversation with the recipient of the call, using my voice (by means of very sophisticated ‘live’ digital synthesis), which leaves the recipient with the idea that the call

was genuinely from me. If this is true, then it is extremely easy to extend this concept to the leaving of voicemails, which the recipient, once again, thinks is me.

Alongside this, there is the concept of the 'Yellow' phone call, where the recipient sees a number on their phone, listed as a missed call, where it appears that someone impersonating me has called the recipient's phone, but hung up before the call is answered, leaving the impression that I had called, but were too 'Yellow' to see the call through.

This impersonation by mobile phone also extends to text messaging (SMS) whereby fake messages, and fake communications cycles can be created, attributed to me.

My own mobile phone (provider GiffGaff, subcontracted to O2) is very likely to be affected by this project in the following possible ways (see Diagrams F and G below):

- firstly, a whitelist/blacklist in operation to prevent certain people (unknown) from contacting me on my genuine number via phone call or text
- secondly, (and this has been apparent in the past) the possibility that if I make outgoing calls, there is always the danger that they will be redirected to a number chosen by the project Central Command, or else the recipient of the call/text will see a false number reported on their device, as if the call/text has come from a different number.
- Thirdly, it is very likely that my genuine phone number (07999 761411) has been cloned using software to allow everyone to abuse using all of the methods outlined in this document, and with the blacklist/whitelist implementation, full control of my genuine number can be maintained by the project

It is not clear if these theories hold any water, but the project is so resourceful and sophisticated that anything is possible.

I have decided to invest in a data-only SIM plan to allow me to both keep my GiffGaff SIM card in my dumb phone (with the number 07999 761411) and also to use my iPhone as a secure (as is possible) internet 5G modem connected to my computer via USB (so that I am not exposed to Wifi interference). I opened an account with Smarty ('Three') for a data-only plan. When I signed up there was a 25-minute internet browser hang, just after I had discovered that my email address (stevekrupa@gmx.co.uk) had already been used to open account with Smarty. This was not me. In order to open *my* account I had to use my gmail email address (opened when I used to have an Android smartphone a few years ago), stevekrupa6@gmail.com. When I had registered this account with this secondary email, on paying for the plan, there was this 25-minute internet website hang. It may be that there were simulations using my secondary email account. I will need to find out from Smarty how it is that my primary email address has been used previously to open an account.

Live Speech (see Diagram D)

My voice (and all audio local to me, such as music I play, or the soundtrack from a film I might watch) – along with live broadcast video of my every activity, as in the film, The Trueman Show, is broadcast on a digital channel (due to implants in my body, put there without my knowledge, and certainly against my will) wherever I am, inside or outside. This means that everyone can hear me live, as they are all fitted with high-technology digital earpieces (covered later in this document). The Security Services may have come to realise that this was potentially a mistake, as I have used the platform to communicate with everybody en masse, ideas which are not to the liking of those who inflicted this technology on me. It is therefore, extremely likely that the Security Services (GCHQ, specifically) have opened a second broadcast audio channel (which I can't hear, but everyone else can) where, using digital synthesis of my voice, they can make it appear that I am saying whatever things they wish to attribute to me, thus deceiving the public into thinking I am talking. The Security Services can do this at any time I am silent (including right through the night) and are also able to switch my channel off, and replace it with their digital synthesis. This allows them to put any words they wish into my mouth.

Body Language

Body is an important aspect of human communications. This is covered in the section describing the role of body implants and Artificial Intelligence. The thing to note is that the AI system is used to produce simulations from every aspect of my body language.

Digital (see Diagram E)

All my online activity, whether it is instigated from a computer using a broadband connection (at home, or in any other locality) or from a smartphone, is extremely likely to be manipulated by the Security Services and their allies in high-technology companies. Diagram E outlines how this is likely to be achieved, with a Virtual Server dedicated exclusively to my online connection (however that might be initiated), which can mimic, using DNS and locally installed server programs, genuine online access, which everyone enjoys. So far example, when I connect to my mail ISP (GMX) either to retrieve emails (using POP3) or to send emails (using SMTP), the Virtual Server takes the place of the GMX POP3 and SMTP servers, and pretends to be them. This means that I never actually connect to those genuine GMX servers, but only to local fake ones on the Virtual Server. The genuine GMX POP3 and SMTP servers are only connected to, by applications on the Virtual Server, allowing Security Services and their allies to censor all outgoing and incoming mail, and to take over, if they wish, communication sessions between myself and the intended recipient, without either of us knowing. They can also instigate new communication sessions in my name without my knowledge, using my genuine email

account. Because I use SMTP, there is no record on the genuine GMX SMTP server of any of this fake activity.

I do not use Social Media, as when I did, a long time ago, it was apparent that it was being abused. However, because of the Virtual Server, the Security Services and their allies can open and use any sort of online account in my name without me knowing, and everybody else thinks it's me. This also true of all my internet browsing activity, which can be faked using the Virtual Server.

I have also used a Mobile Wi-fi dongle in the past for internet access. This dongle (initially from Vodafone but now from VOXI) is extremely likely to also have been cloned, allowing others to abuse internet access and SMS. I last bought a plan on 12th August 2025 but it never became active. I sent an email to VOXI on 1st September 2025 to cancel the plan but have as yet not seen a reply.

All of the technology in my flat (in particular the LG TV, the HP Printer and the Fibre-box for broadband), are very likely to have been corrupted. The TV, when I first used it, kept asking me if I wanted to upgrade the firmware, to which I always answered "No". These requests, however, stopped and therefore I can only assume that the TV had either given up asking (why would it?) or else had done an upgrade without my agreement. The TV has not been connected to the live internet for a long time – and it was only ever connected on a handful of occasions, all of which, aside from one, were for a very limited time. The one occasion where it was connected for some considerable time, was during the Euros when I watched a game on iPlayer. The firewall log trace of the TVs activities whilst I was using it to watch films (not internet-connected) indicated that it frequently tried to access my laptop on port 80. It is possible that the TV firmware was upgraded so as to allow it to operate as a hotspot, and give access to the internet via the possibility of a rogue Fibre broadband box, or perhaps some 'down-the-street' router, all of which was spoofed as if it came from my laptop and down my internet connection.

The HP printer did an unsolicited firmware upgrade at 13:40 on the 19th August 2025, which undoubtedly allowed it to connect to the internet (possibly via a built-in hidden hotspot) using a built-in hidden hotspot in the Fibre box broadband router, or via a 'down-the-street' router, or even via the Smart Meter. I am not aware of any other wireless-internet routes from my flat, but there may be other secret ones hidden.

Between the 19th August and the 27th/28th August, the printer (which was only ever switched on when I wanted to print a letter) went rogue and generated lots of fake activity down the internet, pretending to be me.

I removed the printer and the Fibrebox on 27th and 28th August respectively. The TV has also been removed from activities. All tech is now out of action apart from my dumb phone (07999 761411) which is constantly switched on, and my laptop which has no internet connection of any kind.

On Friday 29th August 2025, I visited Aberdeen central library to register as a user (I had opened an account that day, but had to log in as a guest as my account wasn't functioning) and to use the library computer to do a few necessary admin tasks. I logged in to my email accounts (stevekrupa@gmx.co.uk, stevekrupa-gb@gmx.co.gb and stevekrupa6@gmail.com) through the webmail interface. On gmx, I read my email briefly, (stevekrupa@gmx.co.uk) and modified some of the account settings – for example changed my password, and added my address. I also noted that the ||"Mobile Phone Number" supposedly registered to the

account was some number ending in 736. I changed this to my correct number, save the changes and logged out. Then I logged into the gmx account associated with my webpage, to do the same admin tasks – change the password, enter my address, etc. The website would not allow me to change my password, and kept me that the password was wrong. The only option I had to ensure that I didn't loose control of the account, was to delete it.

I noted above that I had to delete the email account stevekrupa-gb@gmx.co.uk because the password had been lost to me. It may be that it has been this account which has been abused and therefore gmx encouraged me subtly to delete it so that it could no longer be abused. However, the note I wrote above about this still stand. It may have been supporters of GB who were abusing this email address, or alternatively it may have been used by my detractors to rubbish GB – to create the impression that I was not to be taken seriously. Either way the account no longer exists (I think!). I will check.

On 1st September 2025 I went to Aberdeen Library and spent about two hours going through a list of actions, using my laptop and the Aberdeen City Guest login. During some of them (notably the attempt to visit a Polish Book website), everything froze on the browser. It is possible that during this time, there was untoward activity going on behind the scenes. During the two hours I was using the internet in Aberdeen library, it is very likely that there were a number of simulations, mainly directed at Targets. I obviously had no visibility of this, but it was apparent when I left the library that there had been some significant covert activity during this period. Many times, all of the activities of this campaign seem to result in a fake link between myself and the default target.

It is very likely that during both my visits to the library (there have only been those two) my real account was abused by someone else, whilst I was using a guest account. The abuse of my library account may have continued whilst I haven't been present. It is my intention, on my next visit to the library, to request a full log of the usage of my account, and to close it, so that every time I use the library for the internet, I will log in as a guest (on my laptop) and record the session as normal.

I have lost access to both my primary (stevekrupa@gmx.co.uk) and secondary (stevekrupa6@gmail.com) email accounts via POP3 and SMTP. This appears to have been an ongoing development, with some access possible in the past few days and weeks, but now (from yesterday) I am refused access via these methods, and can only access both accounts by using webmail. I am keeping a copy locally of every email I send, but cannot be sure what is happening to my email accounts. Also, I set up an email account with Wordpress for my website but have completely lost access to that.

I am now accessing the internet by using my iPhone with a Smarty (Hutchinson) data-only SIM plan, but it appears that every time I turn my iPhone on, even without using it as a usb-based hotspot, simulations take place. As a data-only system, I obviously (and deliberately) cannot send text messages or make phone calls from it, and I have disabled my email account iPhone service, so I am not sure how I am being simulated using this route.

My iPhone 14 appears to have been completely taken over. At 18:14 – 18:16 yesterday (Friday 26th September) it was apparent that something was downloaded to it remotely, almost certainly by Apple, which appeared to change the Personal Hotspot functionality, at a minimum, probably enabling covertly, Wifi Personal Hotspot functionality, which I haven't been using, instead using only USB hotspot functionality. This change would allow local connection to my iPhone when I was online, and make it look as though I was doing things (such as sending messages) that I wasn't doing. Also, this morning my iPhone switched on

without my intervention at around 0810 and it is likely that messages (probably emails) were sent without my knowledge. My email account on my iPhone is disabled (or at least I disabled it – it may have been remotely re-enabled). I have never been able to see my Sent folder on the iPhone, I suspect deliberately by Apple, so that I am unaware of emails which have been covertly produced and sent from my phone. I have only ever sent one email from all of the three smartphones I have actively owned and used, and this was an accidental sending of a message I had already sent from Inverness library to Acer Technical Support regarding my laptop not working, sometime in the first half of 2024 – if I remember correctly.
It is likely that my iPhone, which I have ONLY been using as a modem for connecting my laptop to the internet (since Sept 17th) is now unusable. I will have to find another way of accessing the internet, or not at all – which I have done in the past, and am quite willing to do so again.

On 24th September at 11:22, GiffGaff sent me a text message indicating that "Immediate Action was required" to ensure that my next goodybag payment went through without a hitch. On my account, apparently I had enabled access to my credit (which stands at something over £5) for the purchase of my goodybag, which normally I pay for by a repeat allowed access to my debit card details by GiffGaff. They warned me that unless I visited their website (my account) by 21:00 that evening, there was the possibility of "issues". I didn't do this, and decided to leave it until the following morning. That evening after I had gone to bed at my usual (ridiculously early) time of 19:45, I got out of bed at 20:38 after hearing noises which sounded like someone trying to access my front door. I had a look and also checked that the attic door wasn't being accessed, but all was quiet, so it is not clear where the noises came from. However, at around 21:10 I detected a change in atmosphere from normal calmness, to something potentially dark and sinister. I cannot explain how this change was noted by me, but I believe that there was a significant project "event" which have involved my mobile phone number at around 21:10 on the evening of the 24th September 2025. It may very well be that the warning from GiffGaff, my postponing action until the following day and the change in atmosphere at 21:10 (possibly from covert and sinister activity involving abuse of my mobile phone number) were all related.

I have in the recent past (beginning of September) used Kismet to analyse what wireless (Wi-Fi) activity there is in the local area, due to the possibility of hostile activity. There appeared to be the fairly normal amount of APs and clients in the neighbourhood, although there were several cloaked APs which I attributed to the likelihood that they were Smart meters for gas and electricity. Yesterday I used Kismet again to scan the local area and found a huge increase in the Wi-Fi activity with a very large number of wireless bridges active, and a significant increase in the number of cloaked APs. There were over 100 active Wi-Fi sites detectable in the local area.

The Wi-Fi sites had (in many cases) associated with them, names of organisations which were quite surprising – including Audi and Apple.

I can only speculate about the reasons for the increase in Wi-Fi sites and in particular for the number of bridges detectable in the neighbourhood. Some of the bridges showed significant levels of traffic which indicated that there is a high level of activity. Bridges are used to link different subnets together, so why would there be the need for so many in the local area? The only reason I can think of, is that the local personal computers and their associated ISPs are linked to form a distributed computing platform, on which can be run CPU-intensive software, such as a powerful AI system. I can not find any other reason why there should be so many local bridges, or why there should be a need to connect so many local computer

systems, with such an intense (in some cases) level of traffic. This is, however, mere speculation and there may well be an innocent reason why there is suddenly such a plethora of devices

I went to the University library today, Tuesday 30th September 2025, to use the Aberdeen City Connect internet (the same one as I have used in Aberdeen library). I chose to use the University library connection because I believed that the students were less likely to be a pain in the arse, as some of the people are in the Central Library.
However, despite the internet connection being up-and-running (I could Ping the gateway and the route from my laptop to the server was correct), I could not access any services. My email client didn't connect to anything and the browser reported no access to the local web server, or any other web server. I tried to get online from 09:53 until 10:04 when I gave up. I was however, simulated twice, I believe, once at 09:52 before I was even online!, and once at around 09:57. I think that both of these simulations went to the default target. It seems, having later looked at the stored connection information from my use of Aberdeen City Connect services at the Central Library, that the connection issue was due to my computer setup, but the simulations were real.
I asked the staff about there being no connection, but was told that they couldn't help. The staff were obviously complicit in being aware of what had happened, and the students (who on the previous day had presented a very different picture to me) I believe had been threatened and told what they had to wear and what they had to do. If their places at university were under threat I can understand why they might go along with being told what to do.
On the way back to the city, there were several students who also displayed the behaviour that they had been ordered what to wear, where to stand or walk, and what to do when I went past. All of this indicates very strongly that the people in control of this project are tyrants and fascists whose only objective is to keep me completely under control, and to destroy my life.
This will not be allowed to happen.

In a world which is so heavily dependent on digital systems, people fail to understand just how exposed they are to abuse of online systems and services. With software in the digital age, anything is possible.

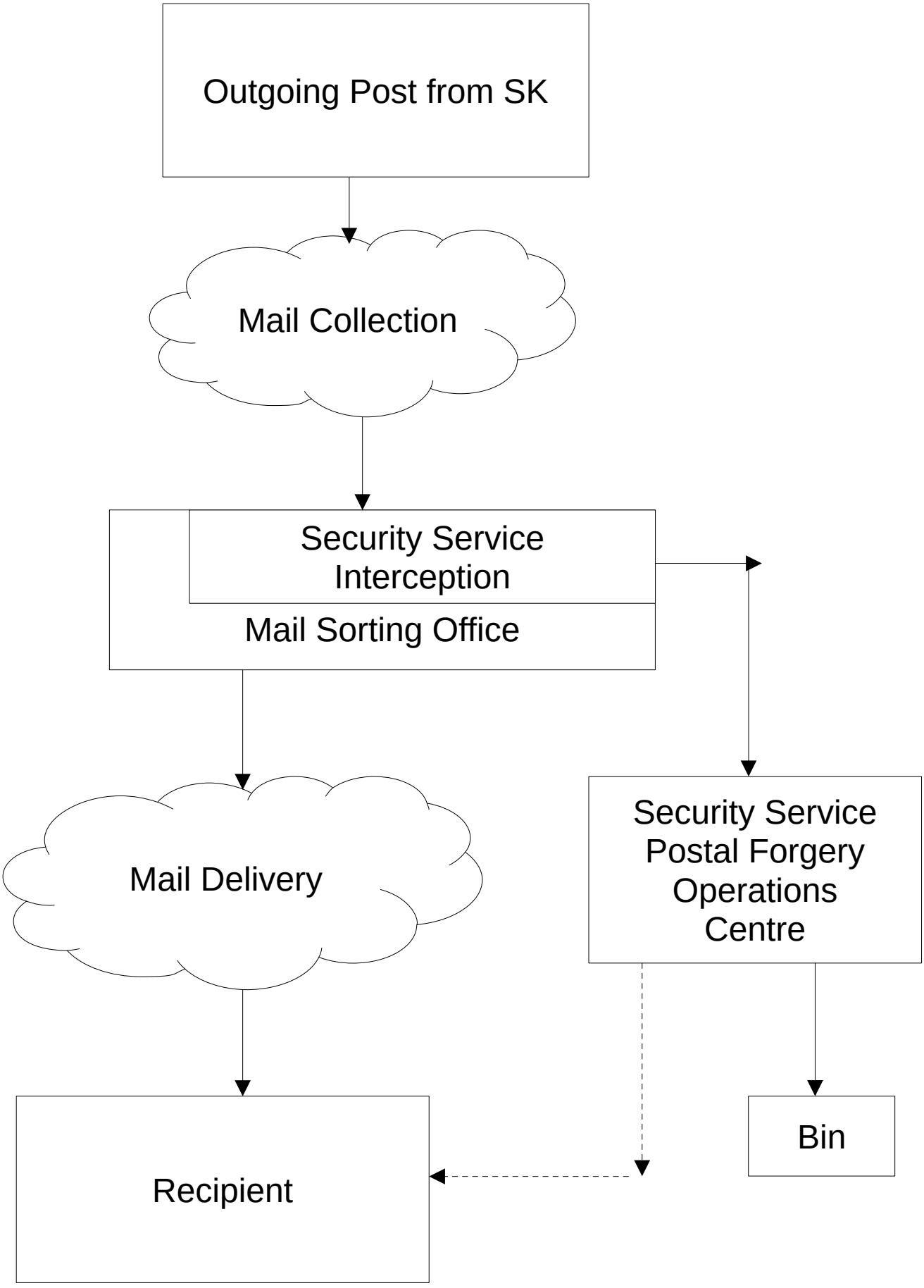


Diagram A : Possible Outgoing Mail Flow

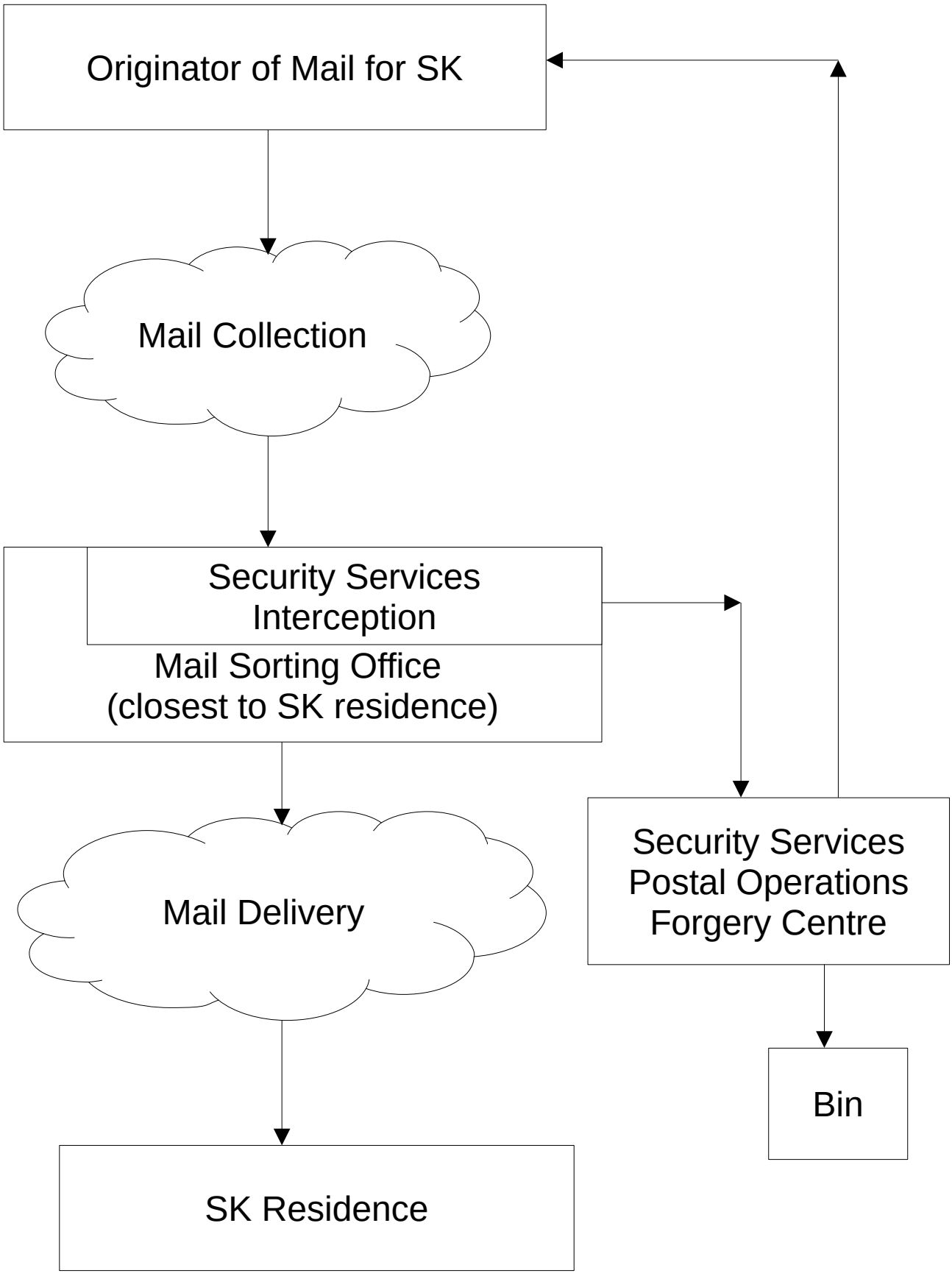


Diagram B : Possible Incoming Mail Flow

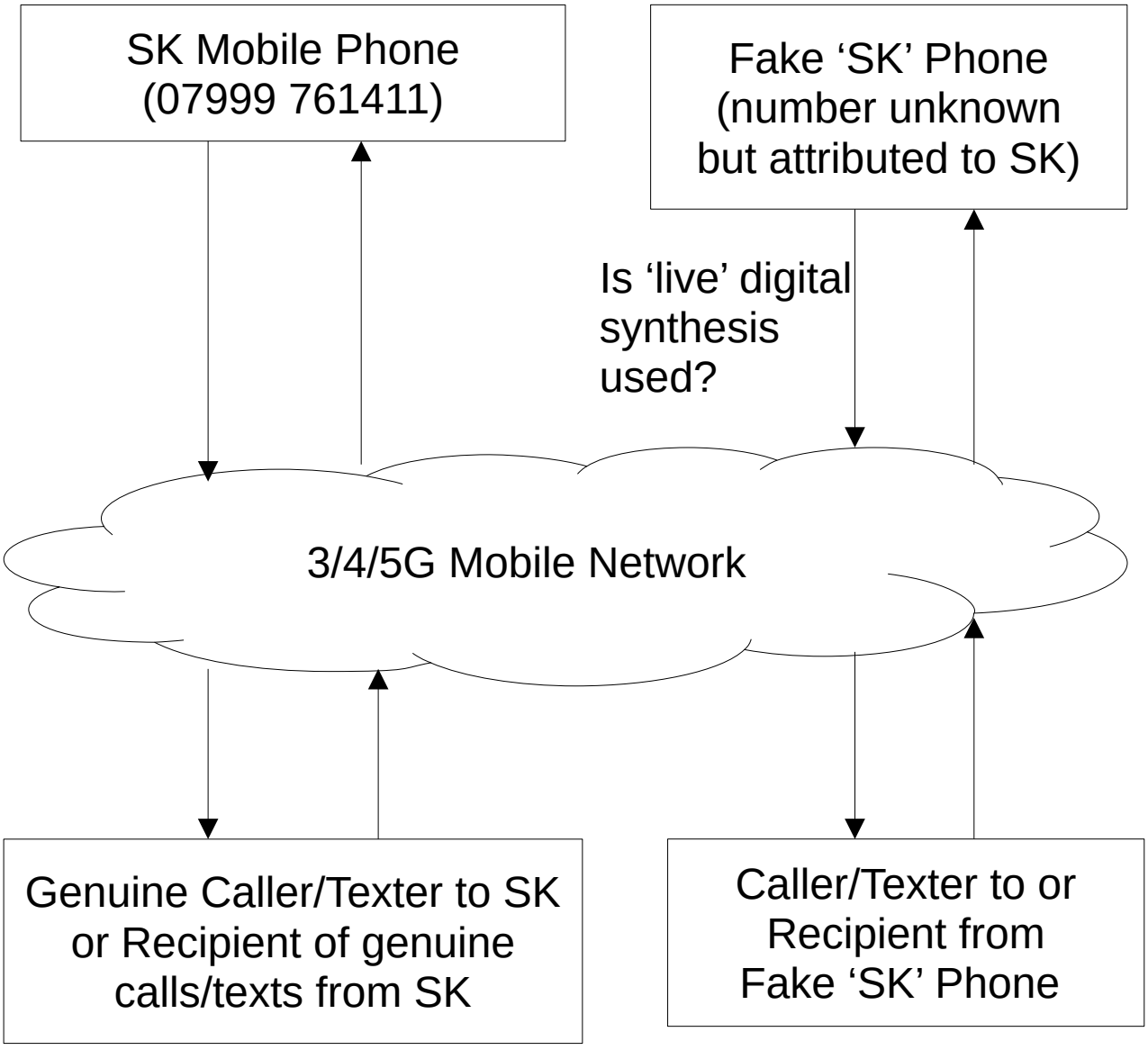


Diagram C : Abuse of Mobile Phone Identity – see Diagrams F and G for more comprehensive overview

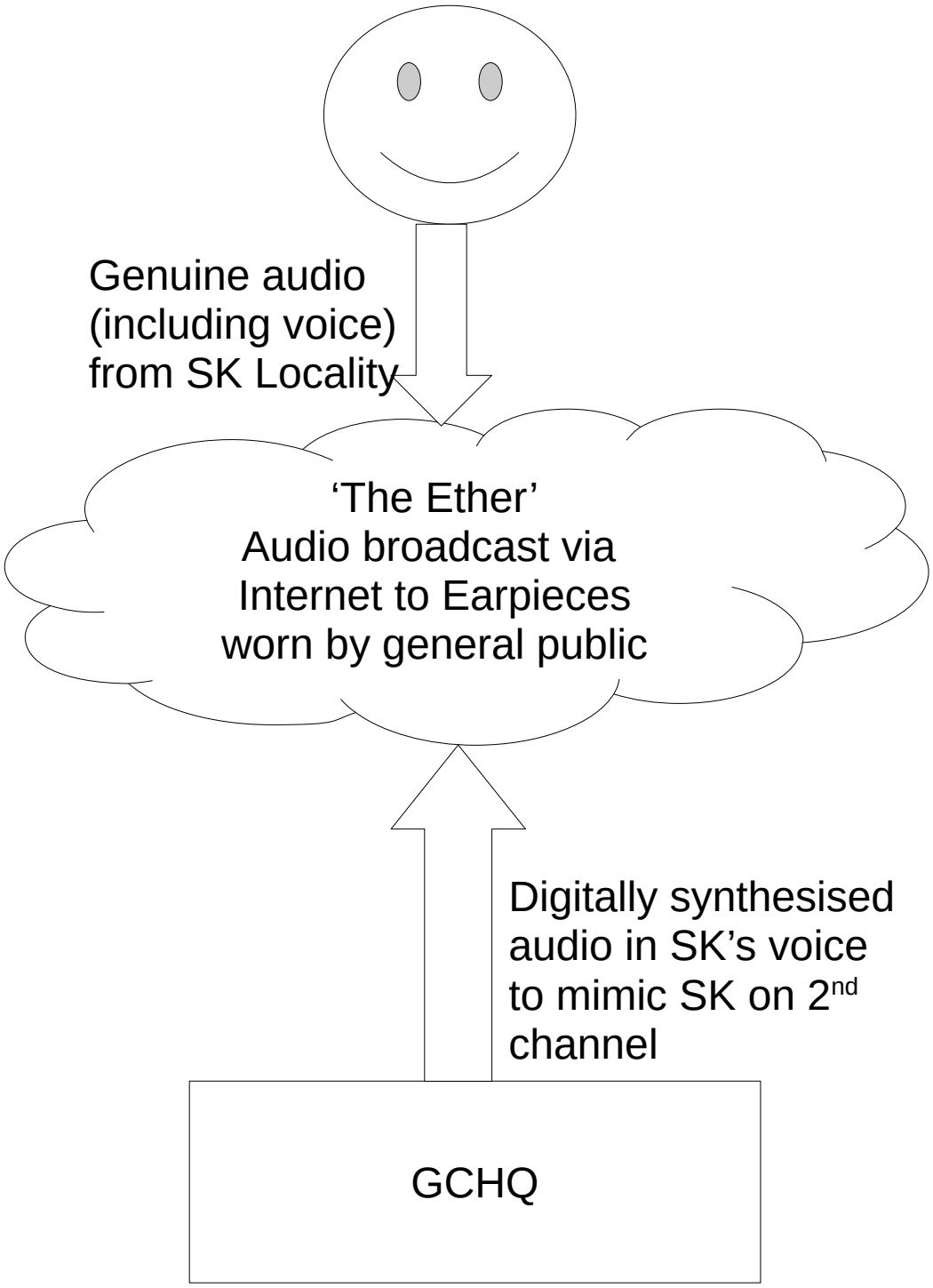


Diagram D : Audio broadcast (genuine and fake)

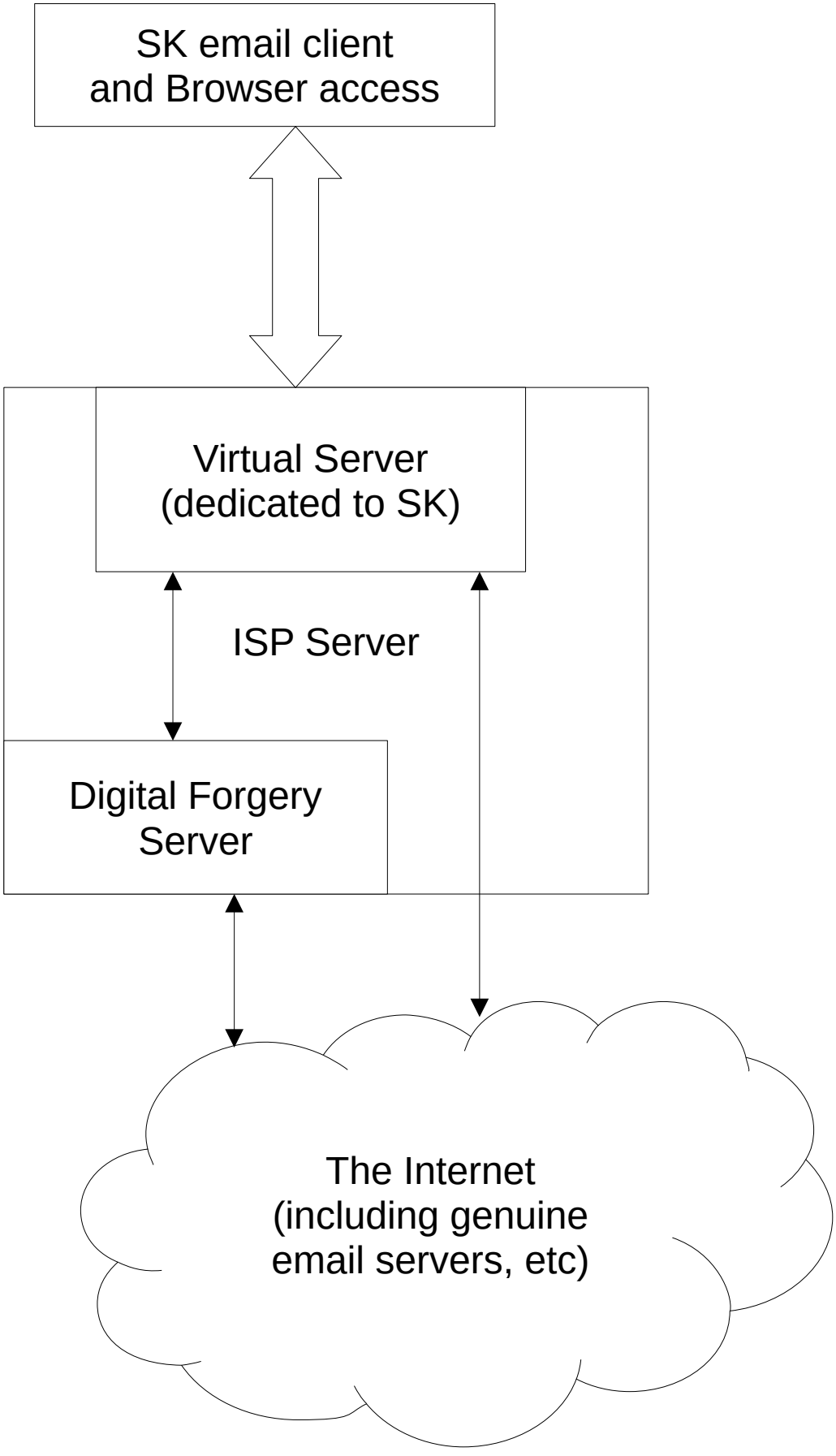


Diagram E : Spoofing email possibilities

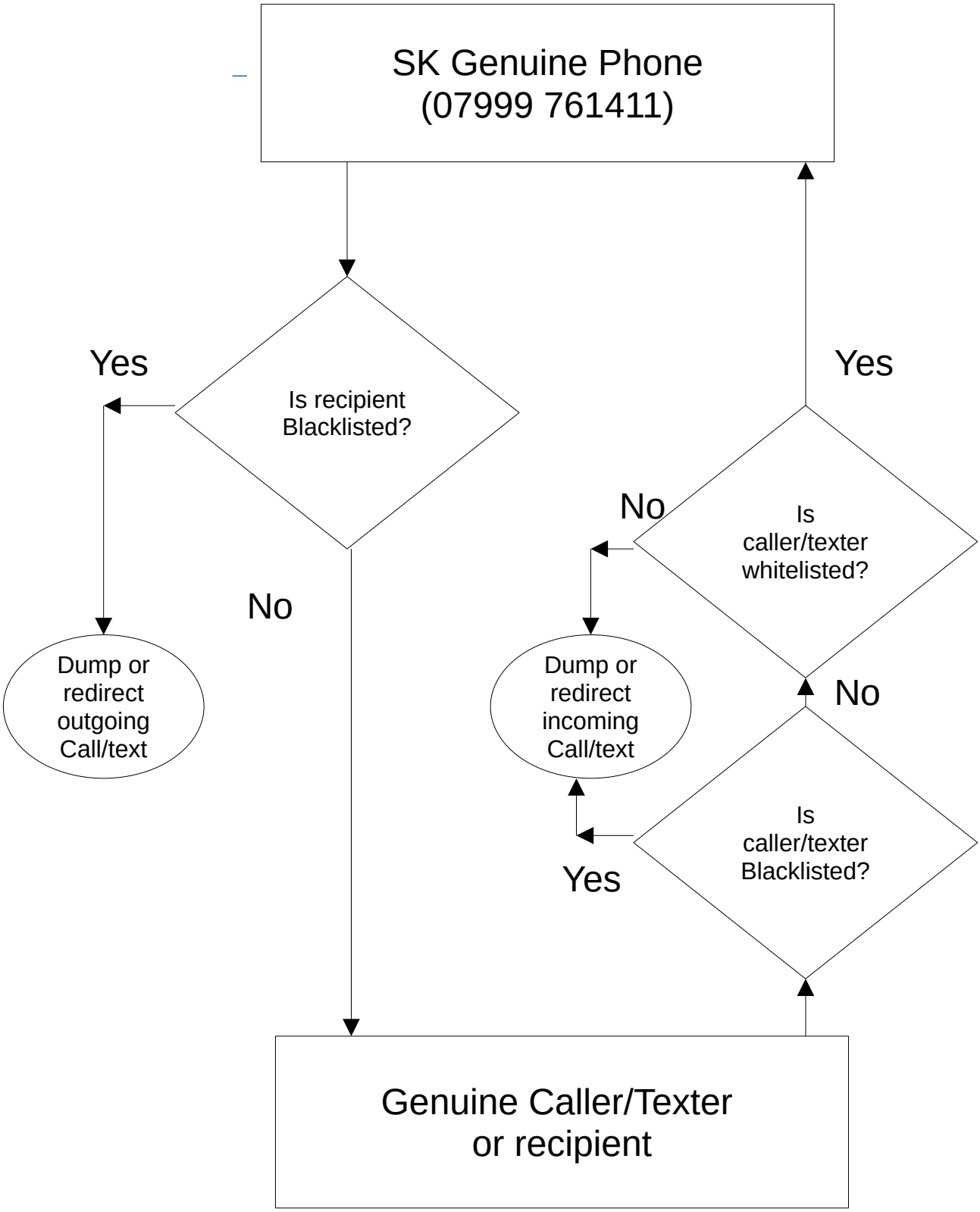
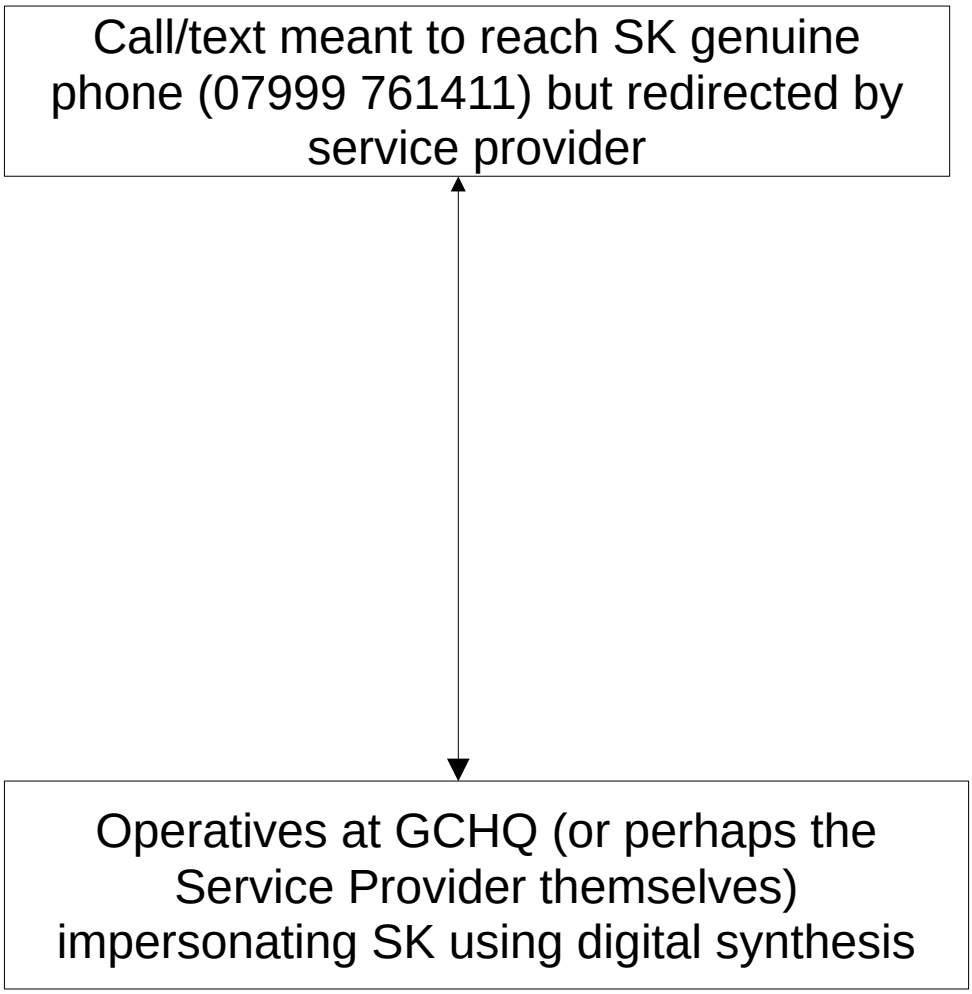


Diagram F: Mobile phone connection interference by service provider



It is unlikely that redirected incoming calls to SK's phone would go to any randomly selected Mobile – who would choose where to send them? It is much more likely that they would always go to the same place, which is likely to be either GCHQ or the service provider themselves.

Diagram G: Redirection of incoming Mobile phone calls/texts by service provider

Conclusion

This project appears to have no ending. It is insidious and disgusting in its character and nature. It is designed, I believe, to provide ‘Blood Sport’ for the masses. The implications of it are incredibly serious and must not be taken lightly.

My war is directed at its exposure and destruction.