ISSN 2348-3156 (Print)
International Journal of Social Science and Humanities Research ISSN 2348-3164 (online)
Vol. 5, Issue 2, pp: (329-361), Month: April - June 2017, Available at: www.researchpublish.com

Here Comes the Bogeyman

Fred Perez

Abstract: **The development of the Web 2.0 and cloud computing has fostered a new era of openness and transparency in universities and colleges across the world: one that enables researchers, students, professors and professionals to work more efficiently, create new models, invent new products, and establish mutually beneficial international partnerships. Serious academic research is now increasingly dependent on ever more complex technologies, such as Artificial Intelligence (AI) and Big Data (BD). But these new information and communication technologies (ICTs) are threatening centralised state controls at various levels, be it privacy, copyright, community management or law enforcement. This paper considers how some Western governments are trying to put an end to this new era of relative openness and global information exchange with extrajudicial measures, programmes of mass-surveillance and investigatory-powers legislation. In the end, I argue that a rational comprehension of these reactionary measures depends upon first situating them within the fear-orienting background framework of the bogeyman.**

Keywords: **Binary oppositions, binarisation, dualism, human rights, equality of arms, surveillance, snooping, desnooping, Bletchley Park, NSA, GCHQ, Prism, Tempora, Edward Snowden, Draft Communications Data Bill 2012, Snoopers' Charter, Investigatory Powers Bill 2015, Investigatory Powers Act 2016, Intelligence Service Commission, UK intelligence chiefs, spy bosses, spy science, proxy, proxies, secrecy, privacy, delusions, psychosis, bogeyman, Hitler, Saddam, Gaddafi, Assad, bin Laden, al-Bagdadi, Mubarak, Kim Jong-un, James Bond, 007, Spectre, Lord Bingham, Lord Hoffmann, Belmarsh decision, Stuxnet, GoldenEye, David Davis, Adebolajo, WhatsApp, Facebook, Lee Rigby, Khalid Masood, Scotland Yard, the Flying Squad, police, anti-terrorism, crime, security, hacking, inside hack, man-in-the-middle hack, digital slavery, Web 2.0, data equality, transparency.**

1. INTRODUCTION

In *Korematsu v United States* [1], the great Judge Patel observed that the Supreme Court's earlier decision (323 US 214 (1944)) 'stands as a caution that in times of distress the shield of military necessity and national security must not be used to protect governmental actions from close scrutiny and accountability.' Even if the events of 9/11in US and 7/7 in UK make it entirely credible that the threat of terrorist atrocities is a real one, evidence, both open and secret, should be shown to the public. After widespread scepticism was attached to the intelligence assessments over Iraqi weapons of mass destruction, who is willing to accept that credible evidence of such plots exist, unless one is invited to examine the evidence?

By protecting governmental actions from close scrutiny and accountability, Western politicians and their secret services are convinced that they are doing their duty. Many politicians are quite charming fellows and many spies are quite moral men. They are not seducers, have no criminal convictions, and would give their lives for Queen and country. Indeed, they are outstanding members of their communities. But they practice 'information debauchery' in a steady, decent way for duty's sake. They avoid situations that might tie their hands. And those who claim association with them or may try to sell their story to the press are easily dismissed as fantasists. There may be many inappropriate relationships, illicit attachments, backhanders and dodgy deals, but they act as if there are not. Pictures are deleted, files are misplaced, secrets are hidden, and silences are bought. And this is not only considered moral, but there is even a matter of national pride attached to it.

[1] *Korematsu v United States* 584 F Supp 1406 (1984) para 21.

Information debauchery does not lie in anything physical; there is nothing morally repugnant in burning a compromising picture or destroying videos of soldiers raping civilians. Such data are removed on a daily basis by the online police. [2] Real information debauchery is both intangible and immaterial, because it lies precisely in freeing oneself from moral relations with the people whose information you classify, destroy, hide, or sell. Such emancipation from the referent is regarded as a merit. And yet Western governments and their secret services should be worried about their delusions gaining traction and meaningful psychotic content via referent-detachment tactics. What if the weaker the evidence, the stronger the case?

I remember how I once worried because British politicians, in particular Tony Blair, did make a huge mistake on the basis of faulty intelligence. Blair's 45-minute claim [3] became the centre of one of my pieces on performative memes. [4] With the adoption of the 45-minute meme as 'true', the uncertainty surrounding Saddam's weapons of mass-destructions was overcome and his bogeyman status was made sense of. The delusional belief was formed on the basis of faulty intelligence or insufficient evidence. And yet it was held with a degree of firmness that was unusual in non-delusional ordinary beliefs that are constantly modified by the intelligence services' validation or refutation. The 45-minute paranoid concern arose in response to certain inner and outer political circumstances, yet we would be none the wiser as to what the world would be like if the bogeyman were still alive. For it was the elimination of bogeyman Saddam which gave a sense of purpose and coherence to the invasion of Iraq. But this sense of coherence, which seemed to facilitate a total lack of guilt, also allowed for the aggrandisement of the hypersalient experience of war as the necessary step for delivering the world from evil. Basically, the world was/is a better place without Saddam.

Years after the invasion of Iraq, Tony Blair was still using the latter argument (that the world was/is a better place without Saddam) to justify his decision. He said he would have invaded Iraq even if he had known there were no weapons of mass destruction – which, being the original reason he gave in parliament for the invasion, it technically constitutes a historical/horizontal approximation to 'lying to parliament'; that is, lying 'in reverse' or 'back-to-front', without relying on the moral verticality of the binary opposition reality/fantasy or the psychotic gap between a paranoid fiction and a reality on the ground which, at the time of the decision, was not clear. Had he lied vertically, Blair would have known that Saddam Hussein really had ordered the destruction of Iraq's stockpile of illegal weapons.

Leaders like Saddam, Gaddafi, bin Laden, Assad, al-Bagdadi, and Kim Jong-un are considered too monstrous to be tolerated by the West. Since the Iraq war, several of these bogeymen have been identified as 'evil' and forcibly removed by Western powers. Even though these leaders are not all the same, US/UK presents them as if they are One and the same [5]: typified cartoon characters, super-baddies that threaten the West with chemical or nuclear weapons. Eliminating the bogeyman is now US/UK's foreign policy – let's say in its relations with other states, both the US and the UK want to have a decisive role in the history of humanity by liberating the world from the bogeyman. Donald Trump says that North Korea is a 'real threat' to the world and warns 'the status quo is unacceptable' in a meeting with the UN security council [6], while British Defence Secretary Sir Michael Fallon [7] is one of the most outspoken defenders of the idea that removing Assad would solve all the problems in Syria. We've got so accustomed to the presence of the bogeyman that, at last, we ourselves really begin to believe that we're all little children and live in a moral world. Very young children, however, can

[2] The UK is the only country in the world with a CTIRU (Counter Terrorism Internet Referral Unit) dedicated to identifying and taking down extreme graphic online material.

[3] On 24 September 2003, the UK Prime Minister, Tony Blair, made the following claim in Parliament: 'Saddam has existing and active military plans to use chemical and biological weapons, which could be activated within 45 minutes'. That afternoon, London's *Evening Standard* carried the headline: '45 minutes from attack'. The following day, 25 September 2003, *The Sun* newspaper had this headline: 'Brits 45 mins from doom'.

[4] I have elaborated on the loss of referents somewhere else. See Fred Perez, 'Guantanamo/Belmarsh and the Horror of Performative Memes' in *International Journal of Social Science and Humanities Research*, 5:2, pp. 187-215.

[5] These leaders are not all the same, as US/UK wants us to believe. Isis' leader Abu Bakr al-Bagdadi, for example, responds to a power typology of leaderless resistance that is made of three distinct components: 1. A hard core of fanatics pushing and trending topics while, at the same time, exercising the functions of policing; 2. Celebrities, microcelebrities, charismatic idols, suicide bombers, and martyrs; 3. Hackers, crackers, and other digital/internet technicians who anonymously administer the systems that keep people connected. This tripartite model of leaderless resistance is quite widespread in today's 2.0 movements.

[6] *The Mirror*, 24 April 2017.

[7] *The Sunday Times*, 9 April 2017.

be very violent but also, and more crucially, very cruel and controlling. It was the great Kierkegaard who first noticed very young children's coercive/controlling use of repetition and their unquenchable thirst for 'such enormous categories that they would now [as an adult] almost make one dizzy. Then one could cut from a piece of paper a man and a woman, who were the man and the woman in general in an even stricter sense than Adam and Eve were.' [8]

It might shock you to learn that the primordial symptom of the US and the UK being 'good' [9] psychotic societies is their infantilisation; their unquenchable thirst for cruelty and repetition, and also for such enormous categories that would make an 'adult' dizzy; a symptom of their social binarisation of state/people as adult/child respectively. With a foreign aid budget, so swollen in 2015 that it accounted for £1 in every £7 given by rich Western countries, British politicians first pretend that the Middle-Eastern warmongering which fills half of their life at Westminster does not exist at all. But look at those unfortunate MPs and at the highest lords and ladies that occupy the House of Lords: the same voting rituals, the same passion for eliminating tyrants, and for costly, investigatory powers legislation that would protect us from the bogeyman.

Perhaps, as David Davis has suggested: 'Because for the past 200 years we haven't had a Stasi or a Gestapo, we are intellectually lazy about it, so it's an uphill battle. Even people who are broadly on my side of the political spectrum in believing in privacy and liberty tend to take the state at its word too often.' [10] Hitler comparisons are always unfortunate. 2017 is not 1945. Trump and Putin are not Roosevelt and Stalin. Angela Merkel is not Adolf Hitler. Yet the question behind this comparison is revelatory, because it is not whether having Hitler would have made us less complacent regarding state surveillance but whether not having had Hitler means that we have to invent him. Saddam, Gaddafi, Assad, Mubarak, how many more have to be compared to Hitler to make the point that 'for the past 200 years we haven't had a Stasi or a Gestapo' – as if we needed to have experienced tyranny in order to recognise it now and to reach against it? The extension of the state of emergency in France, for example, makes French laws more repressive than those approved by Mussolini in fascist Italy. And we should say enough is enough. The world would be a better place not by removing our current bogeyman from power, as US/UK says, but by not reacting like children to him. We blame both Italian fascism and German Nazism for having normalised the state of emergency, and then we tolerate it in our democracies. How can we remain passive before this return of fascistic policies?

Perhaps we're finding the world so changed, so disintegrated, so unrecognisable that we feel the need to invent a bogeyman. Yet, we must be complete deluded idiots because we desire something we haven't had for the last 200 years. Instead of being amazed or saddened by this infantile desire which renders us vulnerable to state manipulation through repetitive memes and such enormous categories that almost make us dizzy, we have considered patiently our leaders' 'war on terror' as a lesser evil and happily have gone on to play our government's lottery in the Middle East, looking forward to a better future one where war is no longer seasonal but a permanent phenomenon in parts of Africa and the Middle East. One where even in the dead of winter, in temperatures approaching −20°C, migrants fleeing war and deprivation are still crossing the Macedonian-Serbian border at a rate of 2,000 a day. One where European member states are unilaterally imposing border controls to stop African and Arab migrants from reaching 'safety' – not only reversing EU's asylum and 'free movement' legal order but also in breach of the Geneva convention that requires all people fleeing persecution and war to be given refugee status. One where the signature policy of the President of the United States of America is the construction of a vast wall along the US-Mexico border. One where history has become too distressing for intelligent and educated people to handle. Perhaps the deluded and the ignorant can cope with this new departure. The trouble with

[8] 'When One is a child, one has such enormous categories that they would now almost make one dizzy. Then one could cut from a piece of paper a man and a woman, who were a man and woman in general in an even stricter sense than Adam and Eve were.' 'Repetition: An Essay in Experimental Psychology' by Constantine Constantius in Soren Kierkegaard, *Repetition and Philosophical Crumbs*, trans. M.G. Piety, into & notes by Edward D. Mooney (Oxford: Oxford University Press, 2009), p. 27.

[9] I say 'good' because group psychosis can have positive outcomes; in the case of US/UK, the psychopathy of One is the glue which holds society together – a society which 'in reality' is split in every conceivable way. Group psychosis can be a way of social cohesion, a way to break out family groups and unite the whole nation from an imaginary point that lies outside the normal universe of everyday existence which I have called I/eye. On the positive epistemic consequences of elaborated and systematised delusions in schizophrenia see Lisa Bortolotti, *Delusions and Other Irrational Beliefs* (Oxford: Oxford University Press, 2010); also useful is her entry in the *Stanford Encyclopedia of Philosophy*: http://plato.stanford.edu/entries/delusion

[10] *The Guardian 2*, 9th November 2015, p. 4.

ignorance and delusion is precisely that if people lack virtue or knowledge, they are perfectly satisfied with the way they are. If people aren't aware that the world around them has become hell, they can't think of getting out of it, for they can't desire the thing which they aren't aware of lacking.

1.1 Draft Investigatory Powers Bill:

One of those satisfying moments of psychotic synchronicity between fact and fiction, between cinema and state, happened when the latest James Bond movie *Spectre* was premiered in London on Monday 25th October 2015 – while articles in *The Times* newspaper over the next four days of the week praised the heroism and endearing normality of the people who work in intelligence and their honest and uncomplicated desire to keep us all safe and free. Some have even suggested that the coincidence between the breathless swoon of the Times man in GCHQ (which run beneath the splash headline 'For your eyes only' [11]) and the release of *Spectre* was a government publicity stunt – though it is difficult to work out who was doing the publicity for whom, whether GCHQ was doing publicity for the Bond movie, or whether the Bond movie was sharing the prestige of the 007 franchise with the beleaguered communications headquarters – throwing its stardust on a desperate bunch of geeks and spooks. But why should *Spectre* take pains to denigrate the senior spook character who wishes to replace the 00 programme with a vast computer surveillance operation, a move that reminds one the recent announcement by Theresa May of new surveillance laws in the Draft Investigatory Powers Bill? Perhaps this is a subtle way of distancing the international franchise from government-abetting. Over its recent outings, it has become clear that the Bond movie franchise is one of those things (like Harrods or Marks & Spencer) whose health reflects the life of the British nation.

The disappearance of the Bond film series would mean the disappearance of the agents on the ground. This is a working hypothesis rather than a theory. For the assumption cannot be tested unless the experiment is carried out. In a psychotic society, TV/film series on so-called essential services like the police, the fire-fighters, the army, the politicians, the doctors, the veterinaries, and so on, are vulnerabilities or national-security risks, for stopping them or tampering with them would cause a massive disruption to the normal functioning of the state. Not only future vocations might be thwarted but also the everyday life of the members of these services, who are dependent on or addicted to their fictional counterparts, would be seriously affected. Their fastidious vocational sacrifices wouldn't be counter-balanced by the vicarious fulfilment provided by the series.

1.2 What is the 'life of the nation'?

Freedom from arbitrary arrest was quintessentially a British value, a freedom enjoyed by the inhabitants of this island when most of the population of Europe could be thrown into prison at the whim of their rulers. Yet, after 9/11, when habeas corpus was suspended for non-British nationals, and powers to detain indefinitely and without trial on mere suspicion were conferred on the government, British values appeared to have been suspended too. The international community has attached widespread scepticism to the existence of 'British Values' since the UK double fiasco over the Human Rights Act 1998 (Designated Derogation) Order 2001 and section 23 of the Anti-terrorism, Crime and Security Act 2001. In their willingness to protect the lives of their citizens from terrorist attacks, the British government nearly killed the life of the nation – in the sense of losing one of their most precious values and constitutional freedoms: freedom from arbitrary arrest and detention.

In the Belmarsh case, Lord Hoffmann, said: 'This is a nation which has been tested in adversity, which has survived physical destruction and catastrophic loss of life. I do not underestimate the ability of fanatical groups of terrorists to kill and destroy, but they do not threaten the life of the nation. Whether we would survive Hitler hung in the balance, but there is no doubt that we shall survive al-Qaeda.' [12] I was delighted to read what Lord Hoffmann had to add to the previous statement: 'The real threat to the life of the nation . . . comes not from terrorism but from laws such as these.' [13] What if certain laws enacted by parliament pose a real threat to the life of the nation?

In Belmarsh, the key question the House of Lords had to decide was whether the get-out clause in the European Convention of Human Rights (Art. 15) applied. Could Art. 5 (the Right to Liberty) be suspended by relying on Art. 15? Two conditions had to be met: 1. There has to be a war or public emergency threatening the life of the nation; 2. If so, the

[11] See 'For Your Eyes Only: The Times goes inside GCHQ'. *The Times*, 28 October 2015.
[12] *A v. Secretary of State for the Home Department* [2004] UKHL 56.
[13] *Ibid.*

state can derogate from the Convention to the extent strictly required by the exigencies of the situation. Of the nine judges or Law Lords (as the House of Lords' judges were known before they moved to the Supreme Court in 2009), eight thought that there was a public emergency that threatened the life of the nation. Even though none of those eight thought that there was a war, they were prepared to accept the government's evidence that the 9/11 attacks posed a global terror threat that was sufficiently likely to affect the UK and, if it did, it was sufficiently likely to be sufficiently catastrophic as to amount to a public emergency threatening the life of the nation. One of the nine judges, however, didn't think there was a war or a public emergency. Lord Hoffmann argued that the other judges had misunderstood what Art. 15 of the Convention when it refers to an emergency that threatens the life of the nation. And I am going to quote Lord Hoffmann here: 'What is meant by 'threatening the life of the nation'? The 'nation' is a social organism, living in its territory (in this case, the United Kingdom) under its own form of government and subject to a system of laws which expresses its own political and moral values. When one speaks of a threat to the 'life' of the nation, the world 'life' is being used in a metaphorical sense. The life of the nation is not conterminous with the lives of its people. The nation, its institutions and values, endure through generations.' [14] In other words, Lord Hoffmann agreed that al-Qaeda might have been a threat to the lives of individual people, but terrorist violence, however serious, does not threaten our institutions of government or our continuous existence as a civil community. Human Rights would be up for grabs if they could so easily give way to other, less fundamental considerations, such as a terror threat. Of course, this doesn't mean that the other Law Lords didn't think human rights weren't important. But they disagreed with Lord Hoffmann about the relative importance of individual rights, on the one hand, and the extent to which those rights should be sacrificed in order to secure other interests, on the other.

1.3 GCHQ/NSA:

Technological innovation can throw up problems for the state. The most talented people rarely want to sit down and obey orders from bosses who force them to spy on others. Many of those who are paid peanuts for sitting in front of a computer all day at GCHQ in Cheltenham are bright vulnerable youngsters. Indeed, the spy agencies entice smart and unconventional recruits, but ultimately do so in support of the future: the informational turn – the fourth revolution in which artificial, synthetic and engineered artefacts are not treated differently from the digital/internet human. In this inhuman and unforgiving environment, young recruits are being subjected to a culture of bulling by bosses for whom even the most basic Web/Net distinction seems dark, mysterious and enigmatic. [15] The head of tradecraft at Cheltenham, for example, was quoted by *The Times* saying: 'If the internet is being used to sell you things, why is it wrong for little GCHQ to use a tiny bit of the data to stop you being blown up on holiday?' [16] The false sense of catastrophic self-aggrandisement betrayed by this comment should be a huge red flag for any psychologist or psychiatrist worthy of their professional title.

But how do you motivate staff if they are stuck on a government organisation whose bread-and-butter activity is mass-surveillance? Instead of getting their sleeves rolled up on new, exciting, outdoors, James-Bond inspired projects, geeks and spoofs are trapped in huge glass cases which should be called 'human industrial farming systems'. Unlike 007, the average GCHQ employee seems grey, shifty, and all too fallible. Most importantly, he is utterly boring. The fictional 007 is assertive, bold, crushing, and muscular. This is the kind of spy that people really want: the fascistic, Nazi-like type. In reality, Bond would be the world's worst spy, because everywhere he goes he's expected. Fast cars, women, weapons, danger, these are Hollywood clichés. Most snooping amanuenses at GCHQ drive Ford Fiestas and Estate Volvos, spend more intimate time with their smartphones than with beautiful women, and don't know how to handle a weapon or how to behave in a dangerous situation. As real spying gets more and more boring, the fantasy of spooks on TV and film grows in appeal.

[14] *Ibid.*

[15] The Net of Internet is not the same as the Web, also known as the World Wide Web. The latter is just one of the services available via the Hypertext Transfer Protocol since 1991. Lower-layer protocols such as the Transmission Control Protocol (TCP) and the Internet Protocol (IP) – used, for example, by Ftp, Torrent, and Skype – are older and not considered part of the Web, although they form part of the Net. The Net is composed of three kinds of machines interacting with each other: mechanical machines such as computers, cables and routers, semiotic machines that generate codes and languages, and biological machines – that is, human beings.

[16] *The Times*, 28 October 2015.

ICTs-based agencies like GCHQ/NSA build their own digital/internet world and, in the process of building it, they lose touch with the reality on the ground. What they deal with on a daily basis are proxies. [17] Despite the paradigmatic importance of their new psychotic modus operandi and their novel dephysicalisation and typification of objects and targets, nothing, not even the biggest fiasco or the death of 'C' would be allowed to change things. When, in the Belmarsh case [18], the government argued that the Law Lords should mind their own business and leave the government and its agencies to get on with the business of making difficult decisions in order 'to keep you and your family safe' [19], the Lords had a clear and straightforward answer: 'things have changed'. Previously, courts had almost invariably been extremely deferential to the government on matters of national security; that is, they had generally been unwilling to second-guess the government when some awkward decision had to be taken in order to uphold national security.

As Lord Bingham put it, the Human Rights Act of 1998 gives the court a very specific and wholly democratic mandate to uphold human rights. In other words, courts will no longer succumb to the argument that national security is none of their business, especially when human rights are at stake. And, against those who have doubts about human rights being a British matter, one can argue that the Human Rights Act of 1998 makes human rights the UK courts' business. Thus public authorities in the UK including courts shall act in a manner consistently with the rights set out in the Schedule to the Act which are the main rights in the Convention. What had changed (thanks to the agency of a few well-educated and far-sighted persons who felt the weight of the yoke and could not restrain themselves from attempting to shake it off – persons such as Lord Scarman, Lord Hester of Herne, and the greater-than-life Lord Irvine of Lairg) was that a neat, coherent if ageing charter of fundamental rights became part of the unwritten British constitution enforceable in their domestic courts. Now, Parliament can revoke the Act, and yet the effects of it would be extremely limited because the UK would still be bound by the Convention. After all, they were the first country to draft it and sign it in 1951. Here we see a momentous constitutional shift in power from the government/parliament to the courts. And this change has extraordinary consequences for ordinary people who may find themselves – for the first time – able to challenge the balance that Parliament has chosen to strike between the rights of individuals and the reactionary agenda of the government and its agencies in matters of national security.

After the momentous Belmarsh decision, the secret services' main priority had shifted from national security to virtual self-preservation. For the agencies' attempt at cybernetic government is now fundamentally apocalyptic. Only the end of the world will bring about their demise. So there is no need for the agencies to tap into the narrative of a self-endangering civilisation that has already predicted its own death by global warming. The ultimate purpose of the spy agencies isn't mass surveillance – which is god-like and thus only possible from an imaginary afterlife – but to mystify and made sacred the entropy and chaos of the world around us. If the ecclesiastics of old days used to scare people with demons and witches, the spooks and politicians of today are trying to scare us with bogeymen such as Saddam, Gaddafi and Assad. If news about the end of the world were one of the most perverse and effective tricks used by ecclesiastics to convert agnostics in the middle ages, the spy bosses of today try to scare the population with the story of one devastating cyber attack whereby an entire city, an entire country and its civil infrastructure can be wiped out by a geeky young man in a back bedroom. Listening to these stories is to live in a Hollywood movie. [20]

Indeed, people must be living in a James Bond film or in Cloud Cuckoo Land not to have noticed GCHQ's three-day advertorial in *The Times* [21] with garrulous pieces by naive journalists anticipating, like a Greek chorus, the tragedy of the Draft Investigatory Powers Bill. The launch of the most invasive surveillance system in the West was glamorised by newspaper coverage praising the heroism of geeks and spooks who are taking on the bogeyman on behalf of a grateful

[17] See Luciano Floridi, 'A Proxy Culture' in *Philosophy & Technology*, 28:4, September 2015, pp. 487-490.
[18] *A v. Secretary of State for the Home Department* [2004] UKHL 56.
[19] A fragment of section 16 (Extremism Bill) of the *Queen's Speech* delivered from the Lords Chamber on Wednesday 27 May 2015.

[20] As the Stuxnet attack has shown, sophisticated cyber-attacks on critical infrastructures can only be done with the help of governments and their secret services. A cyber conflict could be as devastating as a nuclear war, only if governments with unlimited resources intervene. Alan Cumming who played the computer hacker Boris Grishenko in GoldenEye is a Hollywood actor and the character he played is still fictional. The geek-in-his-bedroom cyber-attack is a myth. For Stuxnet see note 54.
[21] See *The Times*, 28th October, 2015.

nation. [22] Right from the beginning, GCHQ is a psychotic fiction but not, for this reason, any less real and vital. Even as the Snowden revelations hit the media, the power of NSA/GCHQ was growing exponentially as the self-appointed regulators of cyberspace, an environment which is essentially ethereal and immaterial – like most of the environments (finance, services, education) that make psychotic societies filthy rich. Geeks and spooks working at GCHQ are colonial heroes for a country without an empire – notwithstanding the BBC, which is virtual colonialism in its own right. And yet, GCHQ, the vast circular building in the suburbs of Cheltenham universally known as the 'doughnut'[23] , seems to speak about the future when in fact (like all imperial buildings) it speaks about the colonial past.

The security services are caught up in a complex temporal paradox. Although prophetic about future terror plots, they only prophesy that which has already happened. Faced with this complex temporal paradox, the young journalists of *The Times* were duped into believing that the new bill was going to make the agencies' work more transparent, more accountable, and more over-sighted by the judiciary. Yet it doesn't take a great legal mind like Lord Bingham's to see that there are loads of holes in that draft bill. The crux of the bill is the surveillance authorisation process. The foreword from the Home Secretary, Theresa May, introduces the bill as a necessary legal instrument to give 'law enforcement and the security and intelligence agencies [. . .] the powers they need to keep us safe in the face of an evolving threat and an increasingly complicated communications environment.' [24] Absent from this text is the question of whether these powers are needed in the first place. But the text is packed with guarantees (particularly at the end of each paragraph) that the powers given to the agencies would be 'subject to robust safeguards and visible, effective oversight'; 'subject to enhanced, consistent safeguards'; 'authorised and overseen'; 'subject to scrutiny and debate'. [25] We appreciate the general idea behind oversight which is no other than a belief that national security must be something other than professional self-limitation. But the accumulation and repetition of phrases around the issue of scrutiny betray the crux of the problem – in the same way as the repetition of certain words by a liar betrays where or what the lie might be.

In the UK, ministers do the approval of the generality of intercepts. Theresa May herself used to do approximately 2,700 a year, before she became Prime Minister. Many critics believe that the authorisation should come from a judge. In order to circumvent the critics' ideal, the writers of the draft bill pulled out one of those back-to-front, perverse tricks, which Nietzsche would have called 'the English kind'[26]. Instead of the judge looking at the potential event before it happens, s/he will look at the actual event after it happens, under judicial review principles. In this way, the content of the event doesn't need to be analysed because the review is always about procedure. Here the test question will be: 'Has the Home Secretary followed the correct procedure?' If so, the judge must go along with it. More diffuse, but not less significant, is the requirement for phone and internet companies to hold communications data for a year. Although the government guarantees that only the data belonging or related to a 'person of interest' would be accessed, it cannot guarantee that the data won't be accessed by a hacker or sold to a third party during its protracted detention in one place. Furthermore, the length of time required (52 weeks) seems quite disproportionate when compared with the length of time for data storage required by other countries. In Germany, for example, it's 10 weeks.

[22] I am referring here to the general indifference of the public to the Investigatory Powers Bill – though I must admit that there is a tiny elite at the top of UK society who cares deeply about it and who opposes it wholeheartedly. The issue of mass surveillance provoked a bust up in the Conservative/Liberal Coalition Government with Nick Clegg blocking the so-called "snoopers' charter". So, over the past couple of years, several independent reviews have been undertaken into the use and oversight of investigatory powers by the Intelligence and Security Committee of Parliament, the Independent Reviewer of Terrorism, David Anderson QC, and a panel convened by the Royal United Services Institute. Between them, they made hundreds of recommendations.

[23] Most of GCHQ staff are now based in their award-winning headquarters in Cheltenham in Gloucestershire. They moved to their purpose-built accommodation in 2004. Popularly known as the 'doughnut' because of its unique shape, the building is so big that you could fit the Albert Hall in its central courtyard. An internal street links all areas. This means that nobody is more than a five-minute walk away, encouraging an informal and collaborative working environment. There is a gym and a choice of cafeterias and restaurants. The institutional wisdom of the doughnut tells taxpayers that spies, if they are to spy, must exercise their dark art in a sacred cathedral-like precinct – cf. Metropolitan Cathedral of Christ the King Liverpool.

[24] 'Foreword by the Home Secretary' in *Draft Investigatory Bill* (OGL, November 2015), p. 1.

[25] *Ibid*., p.1.

[26] Friedrich Nietzsche, 'Preface' in *On the Genealogy of Morality* (Cambridge: Cambridge University Press, 2010), p. 5.

Next on this road full of potholes is section 217 which obliges ISPs [27], telcos and other communications providers to let the government know in advance of any new products and services being deployed, allowing the government to demand technical changes to software and systems. To this (often misguided) attempt to remove electronic protection on encrypted communications by the backdoor [28], we must add other dubious snooping capabilities, such as the power given to the police and security services to record conversations between suspects and the lawyers. This damages principle of 'equality of arms' issued by the European Court of Human Rights as part of the right to a fair trial, under art. 6 of the ECHR. The main worry about recording conversations between some putative terrorist and his or her brief is that it may one day be invoked as sufficient cause to end court proceedings or as grounds for an appeal under art. 6 of the ECHR. Another worry, going back to the first point I made about back-to-front judicial techniques, is that until now the Investigatory Powers Tribunal (IPT) investigated complaints that law enforcement and intelligence agencies had used their covert investigatory techniques unlawfully. The present system is to be superseded by one single authoritative body which 'has all the skills and resources it needs'.

This new centralised system, doesn't it smack of totalitarianism? And the all-powerful single Commissioner with a significantly expanded role in authorising the use of investigatory powers and a wide-ranging and self-determined remit to oversee the protection of covert and secretive investigative techniques, doesn't it remind one the powers of the Grand Inquisitor Torquemada? Imagine, then, that the inhabitants of England find some great Commissioner who shows rare foresight in protecting them in an emergency, rare boldness in defending them, rare solicitude in governing them, and if, from that point on, they contract the habit of obeying him/her and depending on him/her to such an extent that they grant him/her certain prerogatives. Perhaps because the British haven't had a Stasi or a Gestapo [29], a Stalin or a Hitler, they may lack the foresight to see it coming.

Obviously, there is no need to take up arms and start fighting to overcome this Grand Inquisitor, for the future all-powerful single Commissioner can be defeated beforehand by simply giving him/her nothing, by refusing to consent to one's own enslavement. 'It's astonishing how few people take an interest in this country,' David Davis says. 'In every other country in the world, post-Snowden, people are holding their government's feet to the fire on these issues, but in Britain we idly let this happen. We're a country that invented James Bond and we like our spies. We have a wonderful illusion about our security services, a very comforting illusion.'[30] It is therefore the inhabitants of Britain, by their own subjection to the delusion of James Bond, who are not only becoming 'genuine believers' [31] in the secret services but also seem to be deserting their liberties and taking on the yoke, becoming objects of mass surveillance, unsuspecting dupes in their government's poker game.

1.4 Here comes the bogeyman [32]

What if there is no age limit to feel the terror of the bogeyman? Not because it is the bogeyman but because it is One and not Many.[33] Being One means that the people scared by him have been binarised and made childlike, vulnerable to state

[27] ISPs is an acronym for Internet Service Providers – corporate entities offering access to the internet. They provide mailboxes, hosting, transit/transmission, routing, bandwidth deals, peering and, in general, connections for digital online communication. In the UK, for example, BT, Sky Broadband, Virgin Media, and TalkTalk, provide internet access for a monthly fee. They differ from OSPs which are 'free' online Service Providers – such as Facebook, Twitter, Snapchat, AOL, Apple, LinkedIn, Google, Yahoo, and Microsoft. Since the rise of Web 2.0, OSPs have acquired a central role in the management of digital/internet information resources that are crucial for psychotic societies to thrive. I prefer to call OSPs Gafa platforms. Gafa is an acronym for Google, Apple, Facebook, and Amazon.

[28] See note 61, where I explain how Amber Rudd, the UK home secretary, defying the laws of mathematics, suggested the possibility of intercepting WhatsApp's end-to-end encryption.

[29] See note 10.

[30] *The Guardian 2*, 9 November 2015, p.6.

[31] Here I follow Bortolotti in thinking that this 'very comforting illusion' of the British people about their secret services doesn't necessarily mean that they aren't 'genuine believers', and that they can't think, feel or act rationally in line with it. Lisa Bortolotti, 'Delusions and the background of rationality' in *Mind & Language* 20:2, March 2005, p. 189.

[32] 'Que biene el coco' ('Here comes the bogeyman') is the title of one of Goya's *Caprichos*. See Francisco Goya, *Los Caprichos*, Hofer Plates (New York: Dover Publications, 1969).

[33] The psychopathy of One can be expressed as: One/One is to a(=)a as One/Many is to exception/rule. a(=)a can be defined as the relationship '(=)' between 'a' and 'a', where 'a' can be either 'a' or the delusional 'a' which is more like a 'b' and where '(=)' being variable can be anything from 'wanting to be'/ 'more or less equal to' / 'not completely being'

manipulation. Remember when we were kids, how real was the idea of Heaven and Hell? How people were divided into Good and Bad? And how black and white was everything? Well, we are adults now. But the state insists on treating us like kids every time they come up with 'such enormous categories' [34] as Us/Them, friend/enemy, black/white, Christian/Muslim, good/bad, West/East, man/woman, day/night, reason/passion, heaven/hell, native/immigrant, and so on. State-sponsored binary oppositions are part of a strategic governing tactic designed to retain privilege and establish domination over individual lives based on fear, dependence and the deprivation of basic rights and liberties – thus the new political interest in US/UK for finding ways of extending the 'state of emergency' and for magnifying the terror/terrorist threat, so human rights can be suspended. [35]

A Janus-faced democracy is composed of two contradictory and asymmetrical notions of justice, under the state/citizen distinction: one applicable to the state and another pertaining to the citizen. The citizen is always subjected to the rule of law. S/he is not allowed to take justice into his or her own hands. Imagine that your daughter gets raped and killed by her boyfriend, but he is set free on a technicality after a long trial. If you take the law into your own hands and kill the man who killed your daughter, you go to prison for life. This contrasts greatly with members of the secret services. They can kill, torture, rape or kidnap someone and still get away on the bases of 'secrecy' and 'national security'. How can this terrible darkness live side by side with the enlightening certainty of the law?

The modern state was created under the day/night binarisation by the philosophers of the Enlightenment. Unwittingly, they put the modern state apparatus on the side of 'reason', 'day', 'adult', 'male', and the people on the side of 'passion', 'night', 'child', 'female'. The state claims the 'day' which can be read as 'reason' together with 'adult' and 'male', while the people can only seize the 'night' which can be read as 'passion' together with 'child' and 'female'. Perhaps this explains why the people's spontaneous passion (exemplified by the mob – as the loose woman) is feared by the state. With day comes 'clarity' and 'reason' and 'knowledge' and 'information'; with night comes 'darkness' and 'passion' and 'ignorance' and 'lack of information'. The people are kept in the darkness while the state is kept in the knowledge. [36]

And here comes the bad news for the spy agencies: you are binarised [37] like every other thing created in the image of the state. So you are on the side of 'light' and 'day' and 'reason' and 'male' and 'information' and 'knowledge', and while you exist the people will remain on the side of 'darkness' and 'night' and 'passion'. This thing you call 'national security' is just a euphemism for 'ignorance' and 'lack of information'; both are on the side of 'darkness' and 'secrets' and

---

to anything that can be similarly and randomly thought. '(=)' implies that two things cannot be exactly the same unless there is an observer imagining that they are the same. The first [qualitative, a(=)a=One/One] relationship is related to the 'identity' component of the psychotic desire, mania or obsession for total equality as read from the I/eye. The second [quantitative, exception/rule=One/Many] relationship is related to the extreme/borderline 'value' of the psychotic experience. It is about the rarity, uniqueness, exceptionality, oddity, scarcity, and life-changing potential of the psycho/semio experience. The I/eye is the site of sovereignty in a psychotic society; an imaginary point from which the moral code is read/shared and the binarised decision is taken.

[34] See Soren Kierkegaard, *op. cit.*, p. 27.

[35] The kind of law that relates to endangered life and which can return a sense of reality to a society under threat (threaten by its own liberation into the abysm of hegemony) are certain legal measures taken under the 'state of emergency' called by an atmosphere/environment of extreme danger: one which cannot be understood from a legal point of view but from the perspective of 'total' life, from the gestalt of the psychotic.

[36] In the UK, for example, the money that funds the security services comes from the taxpayer. Yet, when the taxpayer's representatives in parliament, the MPs, dare to ask spies questions, they can't even answer because of security issues. Not answering would be morally acceptable if the spies increased people's wisdom through secrecy and silence. How can the British people be so appreciative of spies who are teaching them nothing and making them look bad in front of the world? After Brexit, are the British people eager to learn and generally to increase their knowledge of the world around them?

[37] To 'binarise' is to read binary oppositions from the I/eye. Binarisation is the process by which the human mind can imagine only one side of a binary opposition; that is, the process of gradation, repression, consistency, transparency and value that gives mass to the moral code of a psychotic society. A vital component in the process of binarisation is the reader I/eye. This is an imaginary point from which the moral code made of binary oppositions is read. For example, in a simple code made of binary oppositions headed by good/bad, sun/moon, reason/passion, and white/black, the reader I/eye returns 'good, sun, reason, white' completely ignoring the existence of the other side; so 'bad, good, passion, black' is masked, repressed, downgraded, under-valued, and ignored. For the concept of 'binarisation' see Fred Perez, 'Psychotic Society: An Introduction with a Glossary' in *International Journal of Social Sciences and Humanities Research*, 5:1, pp. 403-418.

'mystery' and 'child' and 'passion'. After all, it is the people's passion for freedom and knowledge that will end up destroying the secret services and their perennial excuse (national security) for 'nonsplaining'. [38] There is a feeling that nonsplaining might be synonymous with taking people for granted in the way they are receiving their services.

Freedom of information requests should be extended to the spy agencies, even if there are people in government who would put this request in the too-difficult box. It is paramount that we explain to men and women and business and the public in general why it is important that the state starts sharing its secrets with the people. Not to do so would be to display contempt, not just for the people's intelligence but for their desire to become grown-ups. For the people have been subjected to infantilisation through the psychopathy of binarisation, neutralisation and depolitisation – which is an opportunity to prove that democratic politics are 'influenced' but not 'determined' by the government and its spy agencies. [39] A crunched, fossilised, limited, sclerotic moral code made of binary oppositions now rules over social relations in psychotic countries like US/UK. Depolitisation and neutralisation sit comfortably on the position of the I/eye from which the moral code is read. A black-and-white, woman-and-man, left-and-right, Easter-and-Western, enemy-and-friend kind of politics is not democratic at all. Missing is the middle ground, which is no longer a space between the binary oppositions, but a point outside this stringent moral domain: it is another field, another dimension, so far removed from everyday life and our enveloped reality, that it stands alone, sucking heterogeneity, being the black hole of the new hegemony, the herald of the TOTAL.[40]

Within all public companies and sectors, the 'spy sector' is particularly shady when it comes to explaining what they're doing. In the UK, for example, Teresa May should be able to explain why her spies were allowed to monitor the web-browsing activity of Britons. ICRs (Internet Connection Records) are not simply the equivalent to an itemised telephone bill, as May described them. They can be subjected to network analysis and contain a wealth of information that telephone bills completely lack. Why should the people be taxed to pay for a service they know nothing about? Either you start sharing your info with the layman or you might not be able to claim legitimacy for taxing those services that remain inscrutable. As we approach the age of hegemony [41], we demand total clarity, total adulthood, total reason, total fe/maleness, total transparency. So, stop your mystifying. Stop your scaremongering. Stop treating us like little kids. Surely, there must be an age limit to be scared of the bogeyman.

1.5 War vs. Wars:

War follows from enmity. War is the negation of the enemy [42]. War refers to the possibility of physical killing. Western democracies have finally found an effective way of deceiving people into thinking that they are carrying on surveillance on their own citizens to protect them from terrorism when all along what they are really doing is to carry on a total war on several enemies: cancer, drugs, waste, obesity, inflation, dementia, terrorism, sexism, racism, organised crime, tax evasion, people trafficking, slavery, hate preachers, paedophiles, homophobes, extremists, and so on. This is neither specific nor exceptional. What these wars all have in common is the cloud – or the warlike method for gathering, sharing, and managing Big Data (BD) in real time; for example, scientists fighting cancer would have a kind of battleground plan

[38] Nonsplaining can be defined as 'to explain nothing to someone, typically a spy to civilian, in a manner regarded as condescending or patronising.' After 'mansplaining', defined as 'to explain something to someone, typically a man to a woman, in a manner regarded as condescending or patronising.'

[39] In his magisterial *Theory of Moral Sentiments*, Adam Smith proved that trade was 'influenced' but not 'determined' by politics. Smith argued that the social order becomes possible by virtue of the restraints which individuals impose upon themselves – not by virtue of the restraints which the security forces put upon the people. Nothing fundamental would change if the secret service or the police disappears. It is this tendency to give importance to secondary or superficial services, to people in uniforms or 'official' things that keeps governments in power. Furthermore, in *The Wealth of Nations*, Smith was bent on destroying mercantilism using arguments that seemed to lend a certain sanctity to the self-interested pursuit of gain, by showing that such activity was productive of benefit to society at large.

[40] In my writings, the TOTAL is a psychotic maelstrom that sucks everything and everyone; the integral information hyperreality we are in – which cannot be challenged with or resisted by conventional means such as revolution, revolt, civil disobedience, street demonstrations, strikes, rioting, and so forth.

[41] Following Baudrillard, the new hegemony is total Evil. Baudrillard says that 'this absolute Evil comes from an excess of Good, an unchecked proliferation of Good, of technological development, of infinite progress, of totalitarian morality, of a radical will to do good without opposition.' Jean Baudrillard, 'The Roots of Evil' in *The Agony of Power* (Los Angeles: Semotext (e) Intervention Series, 2011), p. 109.

[42] According to Spinoza, determination is negation; to consider war, one must determine/negate the enemy.

to manage meta-data or BD in real time. Snowden's data are too static and too directed to particular persons to represent or even approximate any real cloud battle simulation/situation. Isn't it strange that Snowden went for particular bits and pieces of information, mostly from dead data silos and archives? Stealing everything would be counter-intuitive to most people but much closer to the reality of spying than stealing a few bits. My next question is: What was the whistle-blower blowing on? And, more importantly, who was the whistle-blower? I think that the later question, with its neat answer (Snowden), is the most important clue to solve the mystery.

In order for the whistle to be blown you need a whistle-blower, right? Imagine what would have happened had there been no whistle-blower. If you don't know who the whistle-blower is, there is a risk of monstrous embarrassment if it turns out, I suppose, to be the NSA/GCHQ or any other intelligence organisation. Without Snowden there would have been no risk; and this lack of risk would have bother everyone, including non-psychotic nations, because nobody would have claimed responsibility. And the bug wouldn't stop. This whole new idea, I think you can call it 'the bug and snoop tech-complex', is about pretending to accumulate and spread Big Data so massively and so widely that we don't know where it comes from and how it has come to us. Functionally, we shouldn't even know its meaning, because (and is this quite important) it is not illegal for the spy agencies to collect data without you and I knowing anything about it. The Snowden scandal tends to work under the psychopathy of exception/rule. For example, he tells us that the phone of Angela Merkel was hacked. Unless one falls under the celebrity One/Many_exception/rule psychopathic spell, I fail to see how her phone contents should matter to us.

Since the rise of Web 2.0 and cloud computing, we have been hearing reports in the press that police and spooks are facing increasing difficulty in delimiting their competences and in intercepting communications. Was the Snowden scandal a desperate reaction by the secret services to the world going dark on them? The tendrils of data spread throughout a multiplicity of platforms and systems across the world. Are spies drowning in Big Data? Most importantly, are spies telling the truth about the insurmountable difficulties they face when they have to weed out those who are simply expressing extremist ideas from those who may act on those ideas. Identifying future killers in a sea of suspects is not an easy task. At any one time, there will be many hundreds if not several thousand suspects that fit the profile of someone who has already killed before. US/UK's lists contain thousands of names, ranked according to threat level. Often a forewarning in the form of what someone thinks, or what they are overheard saying, would be sufficient to put a new name on the list.

However, it seems counterintuitive to spycraft to listen to gossip [43]. So looking beyond the firewall or having to connect to external partners like the Gafa [44] platforms is quite new to old-school spying. These days, a simple hack would contribute its share in order to drown snoopers in the irrelevances they gather. The blind spot of Big Data (BD) reflects the cultural bias of a society in which technological growth in information management is associated with the accumulation rather than with the refinement involved in mass-surveillance programmes. US/UK's commitment to the compulsory snooping of its own people now reveals itself to be as futile as their pretended commitment to the compulsory deradicalisation of home-grown jihadis.

Yet the promise of these spy technologists that their efforts (if adequately funded) can offer some kind of final solution to the problem of terror, sound as fatuous as the impossible promises made by the prophets and priests of previous ages of salvation in exchange for money. Why? First, let us consider if there is a problem with BD. According to Wikipedia, BD is a 'term for data sets that are so large or complex that traditional data processing application software is inadequate to deal with them. Challenges include capture, storage, analysis, data curation, search, sharing, transfer, visualization, querying, updating and information privacy.' Any reasonable person that reads this definition would be at best mystified and at worst put off by the complexity and insurmountable challenges of BD. Against this self-defeating vision of DB, I would like to argue that the 'Big' of 'Big Data' can be seen as a 'good' thing rather than a 'bad' thing. Who said that having too much of something could be a problem? Of course, if you have too much of something (say, food), you have at least one problem: storage. Similarly, the main problem with BD is that we produce more data than we can keep. This has been explained by a multitude of academics and technology aficionados by referring to Moore's law. [45]

[43] Occasionally, spies do listen to gossip. This may have terrible consequences. For example, the key feature of Tony Blair's 2003 dossier about Iraq's weapons of mass destruction was a claim that Saddam Hussein could unleash weapons of mass destruction within 45 minutes. Adam Holloway, a defence specialist, said that MI6 obtained the 45-minute claim from a Taxi driver who had overheard two Iraqi military commanders talking about Saddam weapons.

[44] Gafa is an acronym for Google, Apple, Facebook, and Amazon. See OSPs.

[45] According to Wikipedia, 'Moore's Law is the observation that the number of transistors in a dense integrated circuit doubles approximately every two years. The observation is named after Gordon Moore, the co-founder of Fairchild

Second, the amount of data generated by the agencies' multiple concerns (drugs, terrorism, sex and people trafficking, organised crime, tax evasion, slavery, etcetera) can give people the impression that they are biting off more than they can chew. The agencies have taken advantage of the generalised (but false) impression that their current computers cannot handle gazillions of data efficiently. The obvious growth of data on an ever-expanding number of concerns has been used as an excuse to obtain funding from their political masters for bigger and better computer systems. It is not a guarded secret that most of those who occupy seats in parliaments are technologically illiterate. Apart from texting and messaging from their smart phones, they hardly know anything about the OSPs [46] they are both using and legislating against. The majority of politicians are seriously out of their depth in their dealings with Silicon Valley companies and spy technicians from their own signals intelligence agencies. Perhaps this explains why it is so easy for Gafa to get tax exemptions [47] and for spy bosses to obtain funding from politicians by portraying cyberspace as a *mare tenebrarum* teeming with all sorts of monsters, from terrorists to hate preachers, from paedophiles to homophobes, and from internet trolls to cyber stalkers.

Intelligence chiefs and politicians have reacted disproportionally and often opportunistically to individual threats with mass-data collections. In US/UK, for example, national security bosses have resorted to the old 'haystack metaphor' to defend their intrusive behaviour and their right to harvest huge quantities of data. US senator Dianne Feinstein famously observed: 'If you want to find a needle in a haystack, you must first have a haystack.' [48] And when the UK chiefs of MI5, MI6 and GCHQ appeared before parliament's intelligence and security committee, a similar observation was made by Sir Ian Lobban, GCHQ director, when he claimed that the Snowden leaks had made it 'far harder' for years to search for 'needles and fragments of needles' in 'an enormous hay field.' [49]

The haystack metaphor is interesting insofar as spies remain ambiguous about what kind of haystack they collect in order to look for the needles within. If these so-called 'needles' are human lives, what is collected, aggregated, compiled, and stored for increasing periods of time, are people's most private records of their most intimate moments. Here information debauchery 'lies in freeing oneself from moral relations with the people whose information you classify, destroy, hide, or sell.' [50] But if these 'needles' are machine-generated data, what is collected is unreadable by humans. So it is beyond 'morals'. Here the success of the 'haystack exercise' would not be achieved by the archiving of all raw data, but by reducing it to smaller, more manageable piles. Standard algorithms [51] would do the heavy lifting first. The raw data must then be reduced to a more manageable size before it becomes suitable for human analysis. Bigger budgets to fund bigger and better computer systems, are only going to exacerbate the problem of spying in the information age by generating more and more data. Instead of more computer power, what the agencies need is (and indeed, they seem to be recruiting) talented individuals [52] who are 'able to spot where the new patterns with real added value lie in their immense databases and how they can be best exploited for the creation of wealth and the advancement of knowledge.' [53]

Semiconductor and Intel, whose 1965 paper described doubling every year in the number of components per integrated circuit, and projected this rate of growth would continue for at least another decade.'

[46] OSPs. Acronym for Online Service Providers – such as Facebook, Twitter, Snapchat, AOL, Apple, LinkedIn, Google, Yahoo, and Microsoft. See Gafa.

[47] The most recent scandal in the UK involved secret talks between Google, HM Revenue and Customs and George Osborne, Chancellor of the Exchequer. Goggle settled for £130 million in 10-year back taxes; this represents an effective tax rate of 3 per cent, considering the company has made about £6 billion profit on UK sales from 2005–15. The UK deal is highly suspicious since it represents a third of the amount of tax that France is demanding, despite Google's UK arm generating about three times as much revenue and employing four times as many people.

[48] The comment was made at the Senate Judiciary Committee's hearing on 2 October 2013, around the time of the Snowden revelations.

[49] In the aftermath of the Snowden scandal, the UK intelligence chiefs, Andrew Parker (MI5), John Sawyers (MI6) and Ian Lobban (GCHQ) gave evidence in public before Parliament's Intelligence and Security Committee (7th November 2013).

[50] See introduction.

[51] Algorithms are mathematical constructs with 'a finite, abstract, effective, compound control structure, imperatively given, accomplishing a given purpose under given provisions.' R.K. Hill, 'What an algorithm is' in *Philosophy & Technology* 29:1, (2015), p. 47. In order to take certain actions and have particular effects, algorithms must be implemented and executed by/into a technology configured for a specific task.

[52] Especially mathematicians and computer programmers who have a natural aptitude for algorithms.

[53] Luciano Floridi, 'Big Data and Their Epistemological Challenge', *Philosophy & Technology*, 25:4, (2012), p. 436.

Regarding the management of Big Data (BD), the paradigm to follow these days is CERN – one of the biggest producer of raw data in the world. The global network of computers known as the Grid that processes and shares BD generated by trillions of collisions in the Large Hadron Collider is composed of thousands of processors working in parallel; a series of Tiers refines the data as it goes along the line. BD is mainly about data reduction. If only 1 per cent of the massive amount of data generated by collision events is selected for analysis, how can the intelligence agencies claim that they need to know 'everything'? This greedy desire for total policing renders the agencies' BD experiment invalid from a scientific point of view. For it is fraught with delusions of grandeur, biases, mirages, and self-fulfilling prophesies. Because of their inability to read BD, what the intelligence services are trying to do now is to predict future behaviour like prophets, that is, to prevent future terrorist attacks by thwarting 'evil' plans before they come to fruition. [54]

The social systems that GCHQ/NSA are analysing are not unlike the particle collisions in CERN, because human group behaviour (like particle behaviour) is subject to unpredictable changes, and unless one knows the future variables, BD can only tell you about the past/present. The intelligence agencies do not have the skills they pretend they have to analyse what's coming in; nor do they possess the intelligence they self-congratulatory assume under the veil of secrecy, which is in itself a reactionary move towards the dogmas and mysteries of religion. The best science by the most intelligent scientists is based on sound evidence, thorough experimentation, and information sharing: data from experiments are shared almost in real time with scientists anywhere around the globe. So why don't the people working for the intelligence services learn something from the scientists and start sharing information?

Having to admit that their intrusive behaviour is causing more harm than good to the world is too much to expect from old-fashioned institutions that are still shrouded in secrecy and mystery. To remain viable, the agencies must survive their operational failures and their irrational mass-surveillance programmes, which so far have been both masked and protected from scrutiny by the James Bond delusion. Perhaps civilians are so overwhelmed by popular culture and the cult of celebrity that they are made to feel that they are sitting at the table with 007 – their fantasy vicariously fulfilled and their egos massaged by the fingers of secrecy. If James Bond is more than a system of meanings, the spying community is more than a system of techniques. Paradoxically, the more attention is focused on information and communication technologies, the larger becomes the symbolic and magical function performed by the fictional 007 and his amazing gadgets. In a psychotic society, the less proof there is that more money spent on computers increases the capabilities of the agencies, the more money will go to the high-tech divisions such as GCHQ/NSA. James Bond makes professional spying tolerable by integrating it into a meaningful setting.

The problem of the symbolic and magical functions performed by James Bond in the Age of Psychosis takes us back to Lord Hoffmann' question: What is meant by 'threatening the life of the nation'? The crucial distinction here is the binarised opposition life of the people/life of the nation. Lord Hoffmann prioritises the life of the nation over the individual lives of its people like, say, one can prioritise the life of men over the lives of women. His argument is that the life of the nation (like the lives of men) is constituted by its institutions and values (such as patriarchy) which are passed on to the next generation. But how would you call the lives of people who want to be someone else, for example, their favourite celebrity? And how can you assume that the life of a nation is the life of its institutions of government and its civil society? A psychotic society can survive without the institution of government but not without its popular culture.

If people can live without politicians, they cannot live without their books, their films, they TV shows, their computer games, their smartphones, their football matches, and their favourite fictional heroes. Politicians are tolerated as 'celebrities' or TV personalities; but their existence is restricted to the world of entertainment only (e.g. Donald Trump): they no longer occupy a 'real' political domain. The political is the new psychotic. The old world of domination has to be

[54] Despite the controversy surrounding the PREVENT strategy, most security forces and their partners recognise the need to develop a 'total' strategy. This strategy sets out clearly that the approach of the UK government is PPPP (Prevention, Provision, Protection and Prosecution). Scary, isn't it? Prevention through awareness-rising, mass surveillance, financial oversight, propaganda, and compulsory education; sending a clear message to potential terrorists that violence will not be tolerated, and educating children and young people on sexual and gender violence. Provision focuses on the delivery of high quality support services for victims and their families which had been inexistent until now and which ensures that those affected by terrorist violence are empowered to improve their safety and re-build their lives. Effective partnership working and information sharing between agencies and informers offer the most comprehensive protection of violence to victims/perpetrators. Finally, there is a commitment to prosecuting perpetrators no_matter_what and ensuring they are accountable for their violent and abusive behaviour.

re-invented as third element, another domain, another system of reference which responds to binarisation under a stringent moral code – similar to the cartoon-like moral code one finds in most Hollywood films, where there is goodies and baddies, right and wrong, macho men and feminine women; where the images might be in colour but the characters are black and white. It is not that the life of the nation resides in the old order of domination, but that even when anti-establishment and anti-austerity protesters kick against it, somehow they end up reinforcing it in predictable, morally coded ways, along the lines of a Hollywood movie. Welcome to 'the psychotic': a process of depoliticisation and neutralisation that turns entertainment/popular culture into the primary life of a nation; a nostalgic Diotima-like invention, third-point reality which can be interiorised and subjectivised because it is crunched and framed by the moral code along/though strings of binary oppositions.

So the 'nation' can no longer be defined *a la* Hoffmann as 'a social organism, living in its territory under its own form of government and subject to a system of laws which expresses its own political and moral values.' First, a 'nation' exists only in people's imagination. It is a concept derived from psychotic patterning in the mind/brain morally coded and binarised through very 'neat' oppositions such as us/them, right/wrong, good/bad, right/left, here/there, east/west, and so on. Second, a 'nation' can no longer be reduced to a *hortus inclusus* or a geopolitical unit within the mass of nations. Mass-migration, emigration/immigration, refugee crises, casual work, corporate work, cyberspace, tourism, retirement, together with improvements in transportation and lower fares, all have made it possible for many people to find themselves in a different country under a different jurisdiction, speaking another language and assimilating new customs. Under the current refugee crisis, for example, European unity is faltering; national independence is becoming an illusion; and the idea of 'freedom' is now rather utopian. Yet these statements are typical of a globalised world where self-government is a chimera. But what a powerful chimera!

1.6 The killing of Drummer Lee Rigby:

Theresa May expected the Investigatory Powers Bill to be enacted as law in 2014 at a cost of £1.8 billion, but Deputy Prime Minister Nick Clegg had already withdrawn his support for her bill as early as April 2013. A month later, following the murder of soldier Lee Rigby in Woolwich on the afternoon of 22 May 2013 in a suspected terror attack, a number of senior political figures called for the bill to be revived. The killing of Drummer Lee Rigby poses a couple of radical questions for the political philosopher to grapple with. First, can one assume that his murder was a 'terrorist' act? Second, what more than a single act of violence, if anything, a government needs to impose and justify an unjust law? The first question can be answered in the negative by referring to the terror/terrorism distinction. [55] But the second question is tricky. Had Christianity not been founded on the suffering and passion of a single man, it wouldn't be that tricky. Historically, the killing of Jesus has been used to justify the perennial oppression of the Jews. The pre-suppositions for this belief are frightening: 1. You need to believe in an homogenised Jewish nation, one that hasn't changed in 2000 years of history – for a multi-faceted Jewish civilisation built on argument and controversy, unity would be utterly artificial; 2. You need to believe in Jesus as God; so the crime is of cosmological proportions. Although we could find more insane compressions and scary uniformities in this example (e.g., monotheism), we just need these two psychotic tendencies of normal human reasoning to surmise that One single killing can be more powerful and significant than Many unless that Many is a number so big, long and neat that it falls under and returns to the power of One with a vengeance; as in, for example, the 6,000,000 Jews killed in concentration camps during WWII.

In the *Charge of the Light Brigade*, the poet Alfred Tennyson reached a one-line conclusion: 'Someone had blunder'd.' One has never been bettered. Everybody in the UK knows who blundered in Iraq: Tony Blair. And everyone in the US knows who blundered in Iraq: George Bush. And everybody in the world knows who is blundering in Iraq and Syria: Barrack Obama and David Cameron, Donald Trump and Theresa May. And looking back to the 'single' cause of these blunders, everyone knows who was behind the 9/11 attacks: Osama bin Laden. And going back in time, who was the 'single' man responsible for the systematic killing of 6,000,000 Jews? Adolf Eichmann. And carrying on with the Nazi theme, everybody knows who started World War Two: Adolf Hitler. And we can go on and on mentioning heroes and villains until the beginning of times. Yet how 'real' a blunder can be when only one person can be blamed for it? One is a

[55] I define 'terror' as a morally coded pornography of representation, whereas I consider 'terrorism' to be mainly about hidden networks of power. The latter can be destroyed by network analysis. The former is indestructible because it is psychotic; that is, it relies on the delusion of a moral code that is common and shared by all members of a society; it is both 'cultural' and 'un-real': How do you destroy something that doesn't 'really' exist?

pivotal moment when one realises history can go in many different directions, many other paths involving democracy and the rule of law, but one chooses to walk down a unilateral invasion of other countries 'just' because (and one reason is enough:) They might want to do us harm.

Having said that, it will always be difficult for those of who hold positions of power to understand what it is like to experience the gravitational pull of One. [56] One's aim is to produce an apparently indestructible, total civilisation. One is hegemony binarised as One against domination. Perhaps this explains why Western democracies are psychotically strong. But hegemony is frightening and evil; like gravity, it's not within our power to resist it. Domination is symbolic. Hegemony is psychotic. One rules over domination from a third I/eye [57] that looks back from the 'outside' (another dimension) onto the moral code of a society. This projection or dissociation of a shared I/eye can only be caused by a sexual trauma of industrial proportions. The state is a rapist and a pimp. Western democracy is coercive pimping and mental rape by the state and its apparatuses. The constant threat of terrorism is the main 'fear' Western democratic states use to create a trauma bond – other fears include immigration (foreigners), financial catastrophe (a new recession), and loss of property (expropriation, repossession, debt). Under One, a) people believe they are in mortal danger. Terror/terrorism is a perceived threat to their integrity – like immigration is a perceived threat to their identity; b) people are treated harshly by the state; in psychotic societies, harsher punishments are interspaced with small kindnesses; c) people are isolated from others – in a situation of voluntary captivity; Western democracies are kidnapped societies made of 'individuals' who are 'equal' units of measurement of the social mass; d) individuals must perceive they are unable to escape; they must live in a capsule which is their social skin. Only through over-taxation (pimping) and universal education (mental rape) can the democratic state re-establish the network of power it has lost through hegemony (mono/psychotic mode) and return back to domination (dual/symbolic mode).

The continual attempts by the government to mobilise public opinion through the use of a single terror event delegitimizes constitutional and democratic authority, while at the same time matches the back-to-front thinking behind all democratic processes which originate in the totalitarian monotheism of Abrahamic religions. As an example of what I mean by 'reverse thinking', we can recall Genesis. The six days of creation are categorising and measuring in reverse: an attempt to explain *everything*; the departing point is a totality, not a beginning; and the beginning is a world already created in the mind of God: a whole. [58] Now, the use of 'reverse narratives' by solicitors and barristers in courts of justice and tribunals across the Anglo-American world is but a secular translation of that heretic interpretation of Genesis. [59] These back-to-front thinking processes are not just partly to blame for the exponential increase of the prison population in psychotic societies such as US/UK, they are also the bases of such contemporary phenomena as fake news, also referred to as hoaxes, propaganda, and disinformation deliberately published on social media sites purporting to be real news.

---

[56] For the psychopathy of One see note 28.

[57] The I/eye is the site of sovereignty in a psychotic society. An imaginary point from which the moral code is read/shared and the binarised decision is taken. Thus the I/eye is a borderline concept: it is the imaginary point of disengagement with 'reality' in a psychotic society which is also the point of moral decision making. The I/eye has two components. The 'I' is an 'identity' component. It is the point of quantitative/qualitative transformation or compression of otherhood into selfhood by accumulation of instances of the same and the similar. So it is the psycho-point that makes you feel superior to other people and also the point from where each side of a binarised relationship can feel superior to the other. In the quest for survival and flourishing, the 'I' strives to maintain and even augment its own delusional power and will naturally be in conflict with the 'Other'. Basically, 'I' is a 'we' that is a 'they' being seen from an 'us'; and the 'eye' component will work that through its lens. The 'eye' is the optical component of the I/eye; a kind of digital lens whose job is to turn chaotic, fuzzy, or distorted reality into crystal-clear images, full of sharp edges and visible details. The affliction of abundance or superabundance of people in a society produces a mental contraction/condition called 'morality'. Individuals acquire existence by accessing the 'moral code' of their society through the I/eye.

[58] In (no time and space) the original pre-big-bang situation, there can be only repetition as One (a=a) thought in the mind of God. Repetition in the physical world works under a different law (a 'wanting to be'/ 'not completely being'/ 'more or less equal to' a) which can be represented, for lack of a better symbol, by 'a(=)a'.

[59] The 'narrative fallacy' allows the jury to rationalise random events by incorporating facts unrelated to the defence's or prosecutor's story retrospectively. Ultimately, whether the accused is guilty or innocent depends on how well a reversed narrative matches its forward mirror image when both are folded on top of each other like a sheet of paper folded in half. Perhaps this explains why courtroom dramas make such a 'good' viewing in cinema or TV and such a 'bad' viewing when they happen for real.

Because a psychotic society is framed by a stringent moral code, the key to fake news is the manipulation of us/them symbols, black-and-white choices and situations, cartoon-like villains and heroes, highly compressed and quite familiar (empty but catchy) phrases or slogans (memes), name calling, and any other nonsensical but highly coherent ideas, arguments, jokes or short thoughts, which can structurally fit a binary oppositional moral code. Here truth as 'absolute certainty' is obtained through the accumulation of instances of the same and similar tending towards the certainty of One [60] ; that is, by online cumulative and refining processes rather than by referent-based meaning. On Twitter, for example, users have become accustomed to compressed (though perpetual) criticism and 'shit storms'. Every day some brainless or maliciously controversial claim receives a load of collective 'shit'. And while the criticism may be justified, it often seems hugely disproportionate to the original offensive statement. Binarisation, asymmetrical equilibrium, and psychotic disproportionality (or asymmetry seen as perfect symmetry from the I/eye) guarantee that online spaces are filled with hatred, racism and sexism. These group of users feel very rewarded when their opinions are magnified online: 'What mighty Contests rise from trivial Things.' [61]

If quarrels over human rights between the judiciary and the executive are effectively masking the psycho-horror of the division of powers, the neat battle over privacy (under the public/private distinction) is masking the distorted face of the digital/internet human. Apart from the horror of reversed narratives, I can see another psycho-horror lurking behind the concept of privacy: the horror of unlimited interconnectivity. Under the non-physical/physical distinction, the loss of control by the national state over transnational flows of information can be equated to its loss of control over transnational flows of migration. State-funded reactions to the former focus on privacy; while state-funded reactions to the latter focus on border controls. Governing cyberspace consists in coordinating transnational flows of information and decisions that circulate almost freely through interconnected/networked sets of codes, machines, and bodies. Current Western democratic governments are making strenuous efforts to control data flows through techniques such as filtering, channelling, draining, and building dams/silos.

They are also trying to control immigration by investing in human dams (Turkey's refugee camps) and building walls (Trump's Mexico wall). Even though these techniques have been symbols of human ingenuity and engineering prowess for millennia, they are more suitable for historical agricultural societies than for current information societies. So when we hear people like Donald Trump saying 'I would build a great wall, and nobody builds wall better than me. Believe me. And I'll build it very inexpensively' [62] , the first problem we face is not the horror of a future dominated by idiots or robots but the traction of a brilliant technical past in the fields of agriculture, engineering and science. We must try to get rid of our prejudices against the new cyberspace and forget what we once thought was true. Let's scrutinise everything. Let's not take anything for granted and be suspicious of politicians who want to build walls and dump immigrants in concentration camps. Let's confront members of the government and other professionals who claim 'they already know'. In such situations, a certain reluctance to leave 200-year-old rituals and superstitions is understandable. What used to be radically advanced has suddenly become obsolete. And what used to be a promise of freedom has become a new form of captivity.

Against such a paranoid/psychotic anti-immigrant, anti-terrorist, and anti-Muslim background, it is impossible not to construct a case for increased vigilance, tighter security measures, and for new anti-terror powers. And yet, the long-awaited intelligence committee report into the murder of Fusilier Lee Rigby (published on 26th November 2014) essentially cleared the spy agencies of failing to prevent the tragedy, placing the blame on one internet company – unnamed in the report but subsequently identified as Facebook. [63] After cataloguing a series of security service failures in dealing with the men responsible for this horrific crime, such as missed surveillance opportunities, delayed investigations, missed chances to reduce the threat based on other criminal activities – ignoring allegations of MI6 mistreatments, kidnapping and dumping dangerous citizens abroad; after all these failures, the committee concluded that only one issue

[60] In his *Treatise on Probability*, chapter XX, on 'Pure Induction', John Maynard Keynes explains stagnation and the limits of growth with elegant simplicity by a mere multiplication of instances increasing towards certainty.
[61] Alexander Pope, *The Rape of the Lock*, Canto I, verse 2.
[62] US President Trump, speaking on 16 June 2015 on the campaign trail.
[63] Blaming of one single internet company for a terror attack has become a pattern in British politics since Amber Rudd, the home secretary, a few years after the Rigby attack seemed to blame WhatsApp for the terror attack by Khalid Masood in London on 22/03/2017. Speaking on the Andrew Marr TV Show on 26.03.2017, Amber Rudd, said that encrypted services like WhatsApp provided a hiding place for terrorists.

had been decisive. That was the exchange, not seen until after the attack, between Adebolajo and an individual overseas (Foxtrot) in December 2012. In this exchange, Adebolajo told Foxtrot that he intended to murder a soldier. Had the spy agencies accessed this exchange, Adebolajo would have been under intense surveillance, with a significant possibility that they could have prevented the attack. The logic of the reasoning is compelling. Yet blaming one internet service provider for the attack is psychotic. Is the government splitting away from reality?

The psychopathy of One overwhelms the real and the physical when the alleged failings of one single technology company (Facebook) can determine draconian legislation while a catalogue of errors by the intelligence agencies is excused. Is it reasonable to expect internet service providers to analyse every message ever sent? Apparently yes. This is as reasonable as expecting British Telecom or the Royal Mail to analyse everything said by phone or post. The conservative government expects internet companies to identify potential suspects by filtering all communications with no warrant or information from the security services. And to do that, they have come up with a piece of legislation that would have made the day of the East German Stasi had they had such brilliant legal minds and more than £2.1 billion a-year at their disposal.

After suffering various changes and emendations, the bill re-appeared in Parliament in March 2016. This was Theresa May's latest plan to grant powers to the state and its secret services to collect the web-browsing history and internet connection records of individuals. First, the main purpose of the bill is to keep pace with the modern world; particularly, with new communication technologies that can cross platforms and international borders, increasingly allowing 'those who do us harm the opportunity to evade detection.' Powers to intercept communications, acquire communications data and interfere with equipment are deemed essential 'to tackle child sexual exploitation, to dismantle serious crime cartels, take drugs and guns of the streets and prevent terrorist attacks'. Second, the scope of the bill is the collection and storage by communication companies of 12 months of everyone's web-browsing history, known as 'internet connection records'. The bill also provides a statutory framework for the police to apply to hack someone's smartphone, tablet or computer – so-called 'equipment interference'. Third, in order to investigate complaints that law enforcement and security/intelligence agencies have breached human rights legislation or used their covert investigative techniques unlawfully, the bill creates an independent tribunal comprised of judges and senior members of the legal profession. They will oversee the use of all investigatory powers supported by a number of judicial commissioners.

This bill was considered urgent because the UK had laws due to expire at the end of 2016 and, according to most MPs, it is better to have a law in this area than to have none. But it is not difficult to see how the polarised purpose of this bill might render it ineffectual. On the one hand, it wants to give more powers to those whose job is to protect us from the bogeyman. On the other hand, it wants to create safeguards for a scared and infantile public. The police and the security services need the powers to do their job, and they will have them. A symptom of the new hegemony is the security services accessing web-browsing records in connection with any crime. This is a welcome development because it goes against the hierarchy of crimes and it sets a precedent to extend equality across the crime/criminal spectrum. But the secondary effect of crime equality is that a motoring offence might be the same as a homicide and the same as anti-social behaviour. Certainly, this can disrupt the measuring techniques which permit the Criminal Justice System to function with a degree of certainty at the moment.

1.7 The issue of austerity:

Many people's dislike of the police and the military translates into democratic governments struggling to raise money for their security services. Desperate measures including declarations of the state of emergency and the magnification of terror threats are often used by democratic governments to entice the population into providing funds for these services. Taxation is a hot political issue at the moment which gives rise to a demand for artificially induced sensibilities, synthetic states of awareness, and an invented consciousness of needs. The Snowden scandal fits into this scenario of general unwillingness by the civil population to fund undemocratic war-related activities in peacetime. In the UK, for example, the mass surveillance revelations by Snowden served as an excuse to bring the bosses of GCHQ, MI5 and MI6 from obscurity to public light. The unprecedented media coverage of the Parliamentary Commission's interrogation of the spy bosses had more to do with influencing the public into believing that the spy agencies are absolutely necessary to the nation's survival than with exposing Snowden as a traitor. But their insistence on the necessity of mass surveillance to thwart terror plots caught up the security services in a complex temporal paradox. Although prophetic about future terror plots that are about to happen (and inevitably happen, 'because we can't stop everything'), they only prophesied that

which had already happened ('yes, we have stopped x terror plots so far this year, but you cannot know the details because these are matters concerning national security'). The Snowden scandal paid off and the £2.1bn funding was secured at a time of austerity when other public services were facing serious cuts. [64]

But what is the taxpayer really paying for? Bargaining power. When psychotic nations like US/UK send their Prime Ministers or Presidents on the Grand Tour to try to get what they want from their European counterparts, they go equipped with chunks of intelligence the European leaders don't know about. Bargaining power is the ability of the US/UK barbarians to have a high degree of influence in the civilised world in exchange for various goods and services. Vital in all negotiations with Europe (which, at the moment, is going through a major security crisis) is fresh intelligence. Apart from the Russians and the Israelis, who have pretty good spying capabilities, the US/UK alliance via NSA/GCHQ is unsurpassable in the rage and quality of the intelligence they provide. So, for example, if you need something from Poland, you come equipped with a piece of information about the Russians. That would for sure impress your host, who would give you something in exchange. Or, when you go to Paris, you give Francois Hollande the names and addresses of those who have just killed one hundred and twenty-nine French men and women. That would give you a few concessions. And when you go to Spain and meet Mariano Rajoy, the Prime Minister, you tell him that there is a plot to kill the royal family he didn't know about. And when you go to Germany, you tell Angela Merkel that her phone has been hacked by the Americans if you are English, and that her phone has been hacked by the English if you are American. This is why it is so important for politicians keep the secret services well funded by the public. Most important, thought, is that the public don't get to know what these services are really for (bargaining chips in trade negotiations). So, now and then, politicians come up with a little distraction or decoy like Snowden to keep the public ignorant but entertained.

Until now, the US and the UK have enjoyed a position of leadership in counter-terrorism measures and policies; this has given them a head start, so to speak, and also a drive to instigate other states to follow their procedures. But, as other states catch up with them, they are beginning to resent their intrusion and interfering. The US and the UK are risking international isolation by pushing their own counter-terrorism agenda through Southern European countries whose culture couldn't further away from the protestant ethic and the spirit of capitalism. These 'puritans' have placed systematic work and the striving for profit at the centre of their lives, and anything that distracts them from that is taken as a threat to 'national security'. Yet, in many of the countries where they have made their presence felt, little else appear to matter greatly, except for family, friendship, leisure and hobbies. Popular culture is the new 'terror'. Until these barbarians from the North learn this simple lesson, their counter-terrorism measures will be condemned to utter failure.

Western leaders are taking unnecessary risks by using these secrets as weapons of acceleration and exchange in international treaties and trade agreements, since the agencies can use that information against them. Take, for example, Fusion GPS in US and Orbis Business Intelligence in the UK. Both companies provide sophisticated cross-border intelligence research services to VIP customers. Orbis boasts of its 'ability to meld a high-level source network with a sophisticated investigative capability'. [65] Basically, 'a high-level source network' means that former spies with a high-level security clearance and with access to classified information, state secrets and other areas of research restricted to the general public, are open to do business with anyone with deep pockets. To put it bluntly, any network that is unaccountable, extrajudicial, hidden and, above all, inextricably dependent on digital/internet information and communication technologies that artificialise, denaturalise, and psychoticise the physical world can be turned against former employers with immunity.

[64] The financial crisis of 2009 ushered a new age of austerity in Europe and America. In the UK, for example, health and education have been the worst affected by cuts. Austerity policies have led to redundancies in schools, colleges and universities, and to courses being closed. The National Health Service in England and Wales has substantially deteriorated in recent years. Local health trusts have struggled to save £20bn from their budgets. 50,000 jobs have disappeared from the NHS. Even though the intelligence agencies' budget pales into insignificance by comparison with the health and education budgets, it is nevertheless the case that, amid sweeping cuts in most government departments, the UK intelligence agencies have received the largest budget boost relative to their size in recent reviews of public spending. When George Osborne presented his review of public spending for 2015-16, MI6, MI5 and GCHQ received a bonus of $154 million, which represents an increase of 3.4% in overall funding for intelligence organisations. While the UK beefs up its security services, it cuts the science research budget, its pollution controls, and its flood controls. It also closes libraries.

[65] See orbisbi.com/our-services/intelligence.

If there is something democratic politicians should worry about at the moment it is precisely their own intelligence services. They constitute an inextricable mesh of transnational and intergovernmental threads which can jump legality with impunity. I believe that the Snowden crisis demands that we review the very idea of publicly prescribed institutional snooping, rather than the methods used in its enforcement. After Edward Snowden's revelations of mass surveillance, it might no longer be enough for ministers and spy chiefs to say "if you've seen what I've seen". Even if this kind of gimmick may invite obedience and submission from a vulnerable, stressed out, pimped, pornified, coercively controlled and mentally reaped population who is still in thrall of mystery and secrecy, it is becoming increasingly tiresome for the intellectual minority who neither feel overwhelmed nor impressed when the mass is sung in Latin.

1.8 The problem of secrecy:

Nothing appears more surprising to those who consider human nature with a philosophical eye than the easiness with which the majority is duped by a minority of government actors and spooks; and the implicit submission with which most people resign themselves to the state-sponsored myth of secrecy. The more one yields to secrecy and to the repetitive incantation about security breaches putting the lives of agents in danger, the stronger and mightier it becomes. The more one yields to the myth, to the mystery and the power of darker forces working within society, the more difficult it is to investigate what's going on. But if these high priests of secrecy are simply not obeyed, they become undone and nothing.

Gradually, and often without entirely realising they are doing so, the spooks and geeks working at GCHQ have begun to ask strange questions and to trace, different, and often less cumulative, developmental lines for the agencies. For example, during the unprecedented, but entirely controlled, access of a journalist of *The Times* to GCHQ headquarters in Cheltenham (at the end of October 2015), one GCHQ official was quoted saying 'GCHQ has to be out there. We can't operate behind veils of secrecy anymore.' [66] The wording of this remark can be broken down into six parts, each of which can be put in the form of a question. (1) Must GCHQ be out there in the open? (2) Can GCHQ operate behind veils of secrecy anymore? (3) Can GCHQ's operations be supported by evidence? (4) Are GCHQ's methods not duplicative of other outdated data procedures? (5) Is the safety and security provided by GCHQ free from harm? (6) Is GCHQ truly necessary? Rather than seeking the permanent contributions of an older (old-school) spy science to GCHQ's present advantage, these questions attempt to display the historical integrity of spy science in our own time. Of course, I am going to leave them unanswered. For what aspects of spy science will emerge to prominence in the course of this desperate questioning effort?

First, at least in order of presentation, is the question of whether GCHQ is necessary in peacetime. Each society defines its own necessities. What is necessary for one might be superfluous for other. Each culture creates its own response to what might threaten its way of life. To postulate a specific kind of threat is a hazardous undertaking, and yet I would venture to reduce the threats faced by psychotic societies such as US/UK to these imaginary three: Islamic terrorism, Russia and populism. The latest populist trend is specifically directed against liberal democracy; particularly Muslims and Jews. Russia and Islamic terrorism are two excuses mainly used to keep the spy agencies on a permanent state of alert and the public on a permanent state of fear. NSA in the US and GCHQ in the UK, for example, will portray themselves as necessary players for the online voting process to be safe and successful. Behind this assertion are recent media reports that Russian hackers have been meddling in other countries' democratic elections. The spy agencies' arguments sport a mixture of inevitability and scare mongering: 'The cyber connections and infrastructure we use need to be safe and secure'; 'The threat has grown from one where we've got to put up a wall that will stop everything to one that is highly sophisticated, where the type of actors has changed significantly and the scale has increased.' In reality, what these agencies will be doing during general elections is spying on voters, producing statistics for the government, and analysing foreign traffic.

Like many big corporations, spy agencies don't spend enough time looking at which individuals (that have control of their systems and networks) could, if they chose to, implement a hack from the inside. The Snowden scandal exposed how vulnerable spy agencies are to whistle-blowers. But they forgot to mention that they were 100 times more exposed to inside hacks. The problem of the inside hack, like the man-in-the-middle hack [67], is that it requires state participation to be

[66] See 'For Your Eyes Only: The Times goes inside GCHQ'. *The Times*, 28th October, 2015.

[67] The attack against Iranian nuclear facility in Natanz in December 2010 was one of the scariest interventions suspected to have been carried out by the NSA in cooperation with developers from the Equation Group. The worm (named 'Stuxnet') was very sophisticated and precise in terms of its ability to target specific devices belonging to the ICS

safe and successful. This is why the notion that Snowden acted by his own volition, completely unassisted, couldn't be further from the truth. In order to be successful, the Snowden hack had to be state-sponsored. His was not the first one attempted by a government employee. Previous whistle-blowers who had supplied evidence of dodgy practices to their superiors or to the media were pleasantly surprised to find out that people in high places were not interested in their information. They were considered traitors. Perhaps they felt guilty and were trying to make amends and do something about it. Secondly, normal whistle-blowers demand anonymity in exchange for information. How it is that Snowden was so keen to put his face on the front page of every national newspaper?

Snowden's stupidity is compelling and perplexing. Here is a brilliant, quiet, polite young man, with his whole life ahead of him, who suddenly makes up his mind that professional spying is an evil thing and the sooner he chucks up his job and gets out of it the better. Snowden is all for the spied-upon civilians and all against their spying oppressors. Isn't this too neat, too one sided? He is fascinated by the art of spying while, at the same time, he hates spying more bitterly than he can admit? Isn't this too binary, too contradictory? In a job like that you see the dirty work of the agencies at close quarters. Isn't this fact intrinsic to a professional snoopers' life far too obvious, too in-your-face to be marked by public outrage? After the Snowden revelations, innocent civilians started to believe that they mattered, that they were interesting, that they could be potential targets. So they got all excited about being in the spotlight. They had not shown much interest in 'real' snooping before. But it was different now that they were all potential terrorists and that anyone could be the victim of a hideous terrorist plot.

The secret services might be wearing a very thin mask: their face grows to fit it with the perfection of a degenerate proxy. To mask the psycho-war status of NSA and GCHQ, the US and UK governments tend to civilise 'terrorism' by making it a civilian matter, so these agencies of war can be tailored-made for the innocent civilian as normal precautionary instruments of self-defence. One thing we learnt from World War Two: the distinction civilian/soldier was purely delusional. So it is within this psycho-narrative of war masked as civilian life that we have to place the mass surveillance revealed by Snowden. That abyss of terror in which civilians are mistaken for soldiers can be happily reversed by referring to the Bletchley Park episode in pre-1945 England .

Despite the futuristic technological impetus of GCHQ, MI5 and MI6, we cannot help but to be moved by mythic images of a bucolic pre-modern England. When Captain Ridley Shooting Party arrived at Bletchley Park, a country house in Buckinghamshire in late August 1938, their members had an air of friends enjoying a relaxed and pleasurable time together. In fact, they were MI6 agents, and members the Government Code and Cipher School (GC&CS), a secret team of individuals including a number of scholars turned code-breakers. The best and the brightest had been recruited from Britain's top universities. Their job was to turn Bletchley Park into a wartime code and cipher breaker location, well away from London. Like so many special teams formed in England and Germany during the war, the team working under Dilly Knox, with the mathematicians John Jeffreys, Peter Twinn, Gordon Welchman and Alan Turing, was framed by the medieval settlement pattern in which urban and rural life had been balanced in healthy symbiosis.[68]

(Industrial Control Systems). By the time it had finished the propagation process searching for the right target, the worm was capable of exploiting various zero-day vulnerabilities and certificates which allowed it to infect all Windows systems. What's incredible to believe is that a secret nuclear-fuel enrichment facility had laughable operating systems designed by Bill Gates, starting from Windows 2000 and all the way to Windows 7 and Server 2008 R2. These are rudimentary systems any kid with a laptop can break into. Even more worrying is the purchasing of vital industrial components from a Western corporation like Siemens who advertises its products on the Internet and which anyone with not much money can buy. Stuxnet found it could search for the Windows systems that were linked to the drives of the Siemens Step 7 SIMATIC software (the world's leading engineering system in industrial automation) for managing PLCs (Programmable Logic Controllers). The PLCs were responsible for controlling the centrifuges used in the uranium enrichment process. These could not be infected by the worm because they were not Windows systems, yet they could be maliciously controlled indirectly by installing a rootkit to modify the booting system of the host in order to remain undetected throughout the propagation method. This might have been a man-in-the-middle attack on the inputs and outputs of the PLCs that control the centrifuges. The worm was possibly brought in one of the ICS components shipped from abroad. Internet infection is also a possibility, though more improbable because of the air-gap that isolated the Natanz nuclear facility. The data about the status of those centrifuges was altered in such a way that, while they were overheating, the administrators thought that they were functioning perfectly well. The end result was the destruction of hundreds of centrifuges and the temporary suspension of the uranium-fuel enrichment programme.

[68] What are the cities of Oxford and Cambridge if not medieval cities inspired by the urban/rural binary which is thought to deliver optimal study performance under quasi-monastic cell-horto-library-praying conditions?

The pre-modern English country-house image, then, was to be realised by a high modernist mathematic rationality. This same contradictory logic that lay behind Bletchley Park lay behind the East/West spatial geography of the Cold War and the James Bond films. What passes today for a reason to never question the existence and purpose of MI5 and MI6 is the assumption that the secret agents who spy for the state could never have any other motive than saving the nation. Spy agencies and secret agents are needed to 'keep you and your family safe' [69]. In Middle Ages, the sovereign's maternal role was emphatically paternalistic too. In reality, secret agents may be necessary to maintain the morale of a nation that relies on secondary self-delusional activity to make or construct primary lives; or lives that seem real but they are not – because they are psychotic. Now, the question remains: why does the British government consider it necessary to endow the three secret agencies (MI5, MI6, and GCHQ) with a 3.4% increase in their combined resource budget, if we are not at war? Clearly, the historical pattern whereby the agencies shrink during peacetime [70] doesn't apply to the present situation. How can one explain this? I can think of two ways of explaining this anomaly.

(1) To go back to the end of World War Two and listen to the punch line of a radio speech given by the head of Britain's new Arts Council, the economist John Maynard Keynes, in the summer of 1945: 'Death to Hollywood!' For people like Keynes, British youngsters weren't just talking American, they were dressing American, walking American, even thinking American. And all this raised the prospect that very soon Britain would merely be a remote colonial outpost of a great American cultural empire. This wasn't completely ridiculous, as Britain had been (around 2,000 years earlier) the outpost of the Roman Empire. Here the conclusion is that Britain has become a colony of the US and GCHQ is just NSA's outpost in Britain.

(2) To visit www.gchq.gov.uk/what_we_do/Pages/index.aspx and click on 'what we do'. Apparently, their main job is to keep the cyber connection and infrastructure we use safe and secure. Also, they play a part in the fight against terrorism, drug trafficking, and other forms of serious crime, as well as providing support to military operations across the world. Basically, they might be fighting several wars at the same time: War on Terror. War on Crime. War on Drugs. War on antibiotics. War on immigration. War on war itself. If the government recognised that 'ours' is a time of war, then explanation for the existence of GCHQ would be unnecessary. But the government is fighting various 'wars' in plural, not fighting a 'single' war – as the psychopathy of the 'war on terror' and the anti-Muslim feeling seem to indicate.

So can the government get away with the lie that we are living in peacetime? Whether it is the war against cancer, diabetes, sexism, racism, homophobia, medical error, heart failure, antibiotics misuse, or whether it is the war on drugs, terror, rape, inflation, unemployment, cigarettes, even the war on war itself, the new economy of total war, which at once encompasses and goes beyond traditional war and its politics of domination/subjection, shares analytical, critical, empirical, and speculative tools increasingly expressed and encoded in digital media and internet. For example, the 'cloud' is hegemonic because the total war that's raging in the world right now makes the 'cloud' its intelligence or brain. But the state cannot accept the hegemonic role of 'cloud' technology and not put a mask over it. Under the old regime of domination, which is the regime of the present government of the US/UK, there can only be One war.

Because there is no war but wars, we must be living in peacetime. If so, the government must argue convincingly why it deems GCHQ necessary. How can its necessity be tested? To trample over fundamental human rights, such as the right to respect for one's private and family life, one's home and one's correspondence, the UK needs to argue that the opt-out clause of the European Convention of Human Rights applies to their current situation. GCHQ's existence/necessity can be tested using Article 15(1) – the Derogation Order of the ECHR. Leaving a state of war aside as it doesn't arise in this case (since the UK government doesn't think that we are in a state of war), the wording of this article can be broken into three

[69] So reads a fragment of section 16 (Extremism Bill) of the *Queen's Speech* delivered from the Lords Chamber on Wednesday 27 May 2015.

[70] Unbelievable, really, that the secret of Bletchley Park should have prevailed until 1974, when *The Ultra Secret*, a book by F. W. Winterbotham, an ex-MI6 officer, revealed for the first time the role of code-breaking in winning World War Two. Shortly after, in 1977, Gordon Welchman took the deliberate decision to appear on the BBC which for the first time on TV dared to reveal the still classified story of Ultra intelligence. 'I don't know whether I should say this,' said Welchman, 'but it seems to me that some of the things have been kept secret too long.' What is clear to me is that the British government, almost bankrupt from the war, was forced to scale back their operations. After World War Two, anyone determined to stay at the forefront of the computer revolution, to build on what the British had already created at Bletchley, had to go to America. The MITRE corporation recruited England's finest brains to develop top-secret research technology.

parts: (1) Is the situation facing the UK a public emergency which threatens the life of the nation? (2) Are the eavesdropping powers and mass surveillance measures strictly required by the exigencies of the situation which has arisen? (3) Are these measures and powers inconsistent with the UK's other obligations under international law?

1.9 Desnooping:

Only in the field of human rights one finds articulate voices demanding the desnooping of society. These belong to a minority of judges who feel strongly about torture and other unsavoury practices by the spy agencies. There are numerous judgements condemning the use of torture and political lobbies have been set up for its prevention. But there is a lack of a cogent argument for the disestablishment of any institution which serves the purpose of compulsory national security. If we are to desnoop, both the tendencies towards secrecy and torture must be challenged. The physical environments where torture takes place must be liberated, and top secret files must be made accessible to the general public. The control of the agencies over snooping equipment increases enormously their cost. Tax-payers should be aware of this. Comprehensive desnooping will require making the artefacts and processes of snooping available to the general public.

The project of desnooping which I propose cannot be limited to the spy agencies alone. Any attempt to reform the agencies without attending to the Janus-faced democratic system [71] of which it is an integral part is like trying to cure lung cancer by extirpating the lung when the cancer has already spread to other parts of the body. Most current snooping reforms are about extirpating cancer-riddled lungs without attending to the rest of the body politic. By large, we should be governed by law but not discretion. And we should be seeking certainty rather than fairness. Since 9/11, successive states of emergency have been temporarily declared in countries such as US/UK whereby a double-faced political system made of the neat democratic mask of rule-of-law domination is ruling in synchronicity with the ugly face of hegemonic chaos. This is subjected to the sovereignty of arbitrary decision making by magnifying the terror/terrorist threat as a case of extreme peril or danger to the existence of the state. Normal people in general don't want to be subject to the arbitrary whim of some autocrat or tyrant. Yet the general consent to despotism in psychotic societies, such as the US and the UK, is surprising and puzzling.

2. INVESTIGATORY POWERS ACT 2016

What does it mean, then, that the Investigatory Powers Bill received Royal Assent on 29th November 2016? It means that the most intrusive and least democratic bill in the history of the UK became an Act of Parliament, following agreement by both Houses of Parliament. In line with what would have been expected from a Stasi or a Gestapo, the Act makes provision about the interception of communications, equipment interference and the acquisition and retention of communications data, bulk personal databases and other information. To put it simply, the aim of the Act is to give the police and the intelligence agencies more powers to survey private communications and internet activity. But, paradoxically, intensive surveillance might turn the police into unemployables. In the same way that intensive agriculture destroyed the subsistence farmer, and the spread of medicine turned mutual care and self-medication into crimes, giving increasing powers and money to spy technologists, while police budgets are cut, might result in the police force being scrapped. [72]

[71] Liberal democracy as technology is a Janus-faced practice/project of domination/liberation. One can argue, following Jeffrey Herf's 1984 notion/book *Reactionary Modernism*, which previously resonates in Adorno and Horkheimer's *Dialectic of Enlightenment* (1947), that the European Union, for example, is conceived as one spatial organism aimed at realising one historical destiny: the joining of a people who (in the past) used to fight against each other; and a unified, endlessly perfectible European space. But this perfect union has come at a price none of us can afford. For the concept of Janus-faced democracy see Fred Perez, 'Guantanamo/Belmarsh and the Horror of Performative Memes' in *International Journal of Social Science and Humanities Research*, 5:2, April-June 2017, pp. 187-215.

[72] Every police force in England faced a 5% cut in government funding in 2015/16 and further cuts after the general election. These cuts came after a reduction of 20% since 2011 in the amount spent by the Home Office on the police. This trend seems to reflect dramatic changes in crime patterns which have seen an exponential increase in economic and online crime. The police force seems unable to adapt to the new information society, a contemporary scene where there is something called 'social media', where a lot more crimes are committed on the internet than in the street, where some people send rape threats on Twitter while others post child pornography or buy/sell drugs and weapons on the encrypted dark web. The other kind of police, the one that deals with internet threats, is not a police force at all, it is MI5/MI6, GCHQ, Scotland Yard, the Flying Squad, and other highly specialised national-security units that are not entirely

The UK secret services are now legally empowered to bug computers and phones, while internet companies are legally obliged to assist them in their spying operations and bypass encryption where possible. This essentially entitles some 48 authorities (including the police, GCHQ, the MoD, the Health Department, Revenue and Customs, and the Home Office) to free reign of your files, whether you are a law abiding citizen or not. As Edward Snowden has commented in Twitter: 'The UK has just legalized the most extreme surveillance in the history of democracy. It goes farther than many autocracies.' [73]

2.1 The three spy bosses:

In the aftermath of the Snowden scandal, the UK intelligence chiefs, Andrew Parker (MI5), John Sawyers (MI6) and Ian Lobban (GCHQ) gave evidence to MPs. [74] The reasons and arguments they put forward for drawing their swords for Queen and Country were at best irrational and at worst monosyllabic. The parliamentary oversight carried out by the cross-party ISC (Intelligence Service Commission) failed to get serious answers from the spy bosses to important questions 'because of security issues'. But their disdain for notions of publicness didn't happened in a vacuum. It came as a result of 9/11 and against the background of the 'war on terror' and within the global context of the rise of a religious-like national security zealotry which indulges belief over reason and hope over expectation. Like the priest and ecclesiastics of old age, the spy bosses assumed an imperial position with regard to other states so that the UK will have a decisive role both in history and in the theophany of delivering the world from Evil. One must assume doxasticism about this paranoid and self-aggrandising delusion. For it is quite irrational and hardly understandable that, under the stress of the Snowden crisis, these intelligence professionals (who were in command of the same services that had been accused of undemocratic practices by the whistle-blower) could presume immunity from ordinary justice under the rule of law. This means that those who are assigned control over our safety automatically cease to be ordinary humans. A different set of rules applies to them.

The entire performance of the spy bosses in front of the cameras took place in an aura of ritualised deference. What we were watching on TV seemed to blur the distinction between the secular and the religious in the sense that the spy bosses were performing a sacrifice by voluntary appearing for the first time in history in front of the public. Their main act of charity consisted in giving away part of their intelligence capital by tapping into their vast wealth of arcane spycraft knowledge. And yet, there they were, the most senior spies in Britain standing like three sahibs with their riffles in front of an elephant they were about to kill. And we, unarmed members of an immense native crowd, were watching the sahibs becoming hollow, posing dummies, absurd puppets pushed to and fro by the questions of the commissioner. For it seems that the condition of their imperial rule is to spend their lives trying to impress us with the magic of their powerful riffles and other awesome capabilities so, in a crisis, the general expectation would be that the sahibs have got what it takes to defend us.

If the goals of national security were no longer dominated by spy bosses and spy agencies, the scope for guess work, mystery and religious zelotry would be more restrictive. Their monopoly on intelligence is no different from the monopoly exercised by the British in colonial India. Colonialism disabled the people of India from doing and making things on their own. It impinged on people's freedom and independence. By developing the image of benevolent caretakers, the spy bosses have reshaped the information environment in the image of the old colonial masters to include an imaginary rogue elephant (the bogeyman), situating themselves in it as the state-appointed sahibs of the internet. 'There cannot be no-go areas on the internet,' John Sawers warned. The reason being that the binary opposition 'real/virtual' must be destroyed: 'We can't have no-go areas in our communities because that allows space for evildoers to

---

subjected to the rule of law. So what are the police resolving? The polarised, binarised, old-fashioned crime, from riots to murders, from attending marches and demonstrations to disappearances, this is what they investigate and nothing in between. The problem with these 'positive' police actions is that they are physical and exceptional in extreme within the general tendency of the infosphere towards dephysicalisation and typification; they are exceptions and attract a certain power from being rare, sovereign and representational, but as the make it into TV series or films, they lose their boring everyday physicality and become part of that hyperreality of dephysicalised, typified and perfectly clonable police officers that we see on TV.

[73] @Snowden, *Twitter*, 9:59pm – 17 November 2016.

[74] On 7th November 2013, all three UK intelligence chiefs were jointly called to account in a meeting of the parliamentary Intelligence and Security Committee (ISC) whose task was to provide political oversight of the UK's spy agencies.

ply their trades and it is the same in the virtual world.' Yet the destruction of the binary distinction 'real/virtual' might expose its darker sister, the binary opposition 'open/secret' on which the secret intelligence service relies for its existence, to an absurd fate: the killing of the rogue elephant by the sahibs was done solely to avoid looking like fools. [75]

Now, when quizzed by the Commissioner on the work of their organisations, answers such as 'our adversaries were rubbing their hands with glee, al-Qaeda is lapping it up' can be less and less tested in a public realm of debate, with evidence marshalled to justify them. Instead, they are asserted as valid not just because the holder *believes* them – which nobody doubts – but also because the public doesn't have the right to demand evidence as they are sacred and mysterious matters related to national security. Rather than showing detailed information pointing to a real and imminent danger to the public, the three spy bosses were allowed to get away with saying that 34 terror plots had been disrupted since the 7th July, 2005, attacks in London. Counting not thinking seemed to be the order of the day.

I wish the spy bosses' stories could have been supported by evidence. I feel there was expectation for more. Responding to questions is easy when you say things people want to hear. Eventually, of course, the public will have to be told. But instead of holding an objective distance, I bet you that people will be drawn in to the James Bond cult. The narrative the spy bosses present is irresistible. Mass-surveillance offers people the chance to be active participants in solving all of the world most horrific murders with one extensive warning: 'Why worry, if you have nothing to hide.' Suddenly, everybody is a potential suspect. How exciting! You are now part of a high-tech and ground breaking experiment where every irrelevance counts.

But the James Bond cult is so awestruck by its own power that perpetrator and victim sooner or later become identical. In the case of a terrorist attack, this is not evident because the aggressor is, according to the spy bosses, 'Muslim' and 'evil'. Yet in the probable case of a nuclear world war, the victim/aggressor equivalence would be immediately evident because the trajectory of social endangering draws a perfect circle: the blast aimed at the victim loops backwards to destroy the aggressor. So far the looping effect of terrorism hasn't manifested itself as a catastrophic threat to life. And however much the spy bosses dramatise the situation by insisting on mass-surveillance as a necessary measure to protect the lives of millions from the destructive capabilities of the bogeyman, it is the adverse effects of terrorist attacks on secondary media, money, property and legitimation that they are really worried about. The destruction and endangering of the tourist industry in Egypt and Tunisia, for example, have the effect of a creeping devaluation of capital and property. Whatever/whoever threatens people in a psychotic society also threatens the property and commercial interests of those institutions (whether financial, educational, medical, political, and so forth) that are parasitic on the capitalist exploitation of the commoditised individual in developing countries.

Perhaps the UK government and its agencies shouldn't underestimate the capacity of the British nation to wake up intellectually in order to analyse, scrutinise, understand, and cope with such oppression. Lord Hoffmann said: 'This is a nation which has been tested in adversity, which has survived physical destruction and catastrophic loss of life. I do not underestimate the ability of fanatical groups of terrorists to kill and destroy, but they do not threaten the life of the nation. Whether we would survive Hitler hung in the balance, but there is no doubt that we shall survive al-Qaeda.' [76] Why a nation that has been tested in adversity by the Nazis and has coped with catastrophic loss of life can't be considered fit to cope with secret evidence and catastrophic news?

2.2 Resistance vs. collusion: the Gafa platforms' dilemma

Let me give you a couple of examples of how the question 'Where?' works in the digital/psychotic era by focusing on how the UK government exploits the state's legal framework to operate mass interception. Where is it? Where is our data? On Tuesday 17th June 2014, the UK government's top security official, Charles Farr, said searches on Google and Facebook, Twitter and YouTube, as well as supposedly private messages on social media among UK citizens can be monitored because they are legally judged to be 'external communications'. Technically, this is absolutely correct: they are 'external' (beyond the UK borders) communications. But, at the same time, if we refer to that famous metaphor of the internet as a big bubble computer inside which we all live, there is little truth in saying that searches on

[75] See George Orwell, *Shooting an Elephant and Other Essays*, Introduction by Jeremy Paxman (London & New York: Penguin, 2009).
[76] *A v. Secretary of State for the Home Department* [2004] UKHL 56.

Google/Facebook/Twitter/YouTube are 'external communications'. It is this sort of loophole in the legislation, which allows democratic states to Big-Brother us, that needs to be put to the test of the question 'Where?'

An information society is a 'query society' that returns positive results when asked the question 'Where?' Because we are as good as our queries, we must keep asking the question 'Where?' to test digital/internet systems for traces of real value. First, we must ask: 'Where are the sensors?' Every corner of the earth is expected to be fitted with a sensor of some kind. The tiny computers in mobile and smartphones, tablets and laptops, video cameras and car sensors turn the world around them into data. If we happen to be in that world, we cannot know when, where or how information about ourselves is recorded. Second, we must ask: 'Where are the copies?' The copies are everywhere. Computers are data-copying machines. Basically, they replicate every piece of data they use. So the internet is a network of copying machines. Because the copying process happens exponentially and regardless of 'copyright' laws, people cannot know where, how or where their data are. Third, we must ask the following question: 'Where is the learning algorithm?' Again, the query returned the psycho-answer 'everywhere'. How can we analyse huge masses of information, the same information we cannot control? Forget trying to understand raw Big Data: every irrelevant piece of info can be recycled into something of mayor importance thanks to algorithms. Say, people's birthdays. Innocent automatic well-wishing notices of 'happy birthday' are posted daily by Facebook and Twitter on behalf of their users. DOBs are important ID components which pose a danger to all those who want to travel the web anonymously.

The first characteristic of internet users' experience is that they are *not* where they seemingly are. While online, users are 'inforgs' (informational organisms) that 'inhabit an infosphere increasingly boundless, seamless, synchronized (time), delocalised (space), and correlated (interactions). It is an environment based on the gradual accrual and transmission semantics through time by generations of inforgs.' [77] Further, within the binary opposition 'external/internal', only One ('external') can be legal. Precisely, under RIPA (Regulation of Investigatory Powers Act) traditional interception of 'internal' communications within the UK requires an individual warrant. Yet the UK is the only country in the world with a CTIRU (Counter Terrorism Internet Referral Unit) – a 24/7 law enforcement unit, based in the Metropolitan Police, dedicated to identifying and taking down extreme graphic online material as well as material that glorifies, incites and radicalises. In an average week, CITRU removes over 1,000 pieces of content (80% being Syria/Iraq related) that breaches the Terrorism Act 2006.

As global industry players like Facebook, Google, Yahoo and Twitter begin to resist being bullied into submission by the likes of the UK, the 'external' side of the binary becomes an ungoverned space. Now it is the turn of the 'internal' side of the binary to be subjected to government's pressure. In November 2014, the UK's major Internet service providers – BT, Virgin, Sky and Talk Talk – committed to host a public reporting button for terrorist material online, similar to the reporting button which allows the public to report sexual exploitation. They also agreed to ensure that terrorist and extremist material is captured by their filters to prevent children and young people becoming radicalised. The strengthening of filters, the facilitation of reporting, and the increasing governmental pressure on businesses/the public to become more proactive, more vigilant, all have the hallmarks of totalitarian politics. Those who don't use Google, Twitter or Facebook are automatically suspected of having something to hide. Internet service providers and social networking sites expect total transparency from their users. Analogic governments, such as Theresa May's, have struggled with this contradictory asymmetry of the digital/internet world in which total transparency is expected from users while total secrecy/mystery from internet providers, the government and its spy agencies, is allowed.

From Part 1 to Part 5, the Investigatory Powers Act 2016 establishes general privacy protections, lawful interception and retention of communications, and equipment interference. The first problem with words such as 'privacy', 'interception', 'retention' and 'interference' is that they belong to the analogic pre-digital/internet age – and the authorities haven't noticed? This type of vocabulary would have been relevant ten years ago, when computer users struggled to organise their files *in* their own laptops and computers. Then, information and programmes resided in that piece of hardware we call 'personal computer'. Yes, the laptop was yours, and there was a sense of 'privacy' associated with personal contents which could be tampered with. Today, however, the idea of 'personal computer' has ceased to exist as every piece of computer hardware serves almost exclusively to give access to the Web and its services. Web 2.0 applications are capable of substituting any software created for laptops, tablets, smartphones, and computers.

[77] Luciano Floridi, 'Web 2.0 vs. The Semantic Web: A Philosophical Assessment' in *Episteme*, 6:1, February 2009, p. 35.

2.3 Privacy:

If privacy means the 'right to be on your own', the digital/internet user is never alone. Web 2.0 users have no privacy. Logged-in internet users are constantly monitored by people, machines, and third party agents. They are never alone with the people they are intentionally communicating with. If mass-surveillance is the normal and banal default position of the commercial Web, why is the UK government insisting on protecting something ('privacy') that doesn't really exist? Any digital machine capable of accessing the Web 2.0, immediately gives the following information away: 1. Name of manufacturer; 2. Geographical location; 3. Type of software used by the machine; 4. Digital identity of the user of that machine, online habits, criminal profile, associates. Users cannot see who or what is monitoring their every move; nor can they tell 'where' their files and applications are. Neither can the government. So their threat or warning of 'interception', 'retention' and 'interference' is as spurious and unreal as their confusion/delusion over 'privacy'.

As a digital/internet user, you don't owe or possess anything that could be called yours. Absolutely everything is owned by and shared with the big corporations that give you free access to their services. So we come directly to the heart of what has undermined the Web: a few corporations maintain, manage, control and profit from your online experience. The Web 2.0 is the turf of a handful of private companies which I call 'Gafa' (Google, Apple, Facebook, Amazon) and their associates. If these services are free is because you are not. You are a voluntary slave. You can't wait to publish, label, comment and link your pictures, videos, tweets, texts in the *mare nostrum* of social media. Digital slavery refers to a condition in which your on-line labour is owned by others, who control, manage and trade with the information you produce. A digital slave is a human being classed as data property and who works for nothing. A chattel digital slave is an adult internet user whose children and children's children are automatically enslaved by the information they provide online, which can be bought and sold. Digital slavery is supported and made legal by the UK government through legislation such as the IP Act 2016. [78]

2.4 President Obama and the rise of hacktivism:

On 19th June 2013 President Obama delivered a speech at the Brandenburg Gate in Berlin. The image of a great man standing behind a wall of bullet-proof glass delivering a speech to the wall in incomprehensible American jargon may be taken as a metaphor of the US's position in world today. For 'zero' is a position not a number – otherwise, there would be 'minus zero'; and, as there isn't 'minus infinite', there cannot be 'infinite' except in the binary opposition 'infinite/zero' as One among other binaries within the stack headed by good/bad, abundance/scarcity, hope/hopelessness, ambition/pessimism, belief/distrust, etcetera. Without their invisible wall of nuclear warheads and their worldwide control of satellite communications, internet service providers and bully corporations, the US would have become 'zero' (would have been destroyed) years ago. As support for the US and its ally the UK was waning in Europe, Obama spoke of a city divided by a wall: 'No wall can stand against the yearning of justice, the yearnings of freedom, the yearnings for peace that burns in the human heart'. Perhaps he sensed a new world configuration in which the US and the UK stood together and alone against the rest of humanity.

Almost fifty years after President John F Kennedy's celebrated 'ich bin ein Berliner' speech, Obama reminded everyone that he had a stockpile of 4,650 nuclear warheads, and that Russia had a stockpile of 4,500, and that they should be holding talks to reduce their stockpiles to the level at which it is possible to avoid total destruction, as if to distract our attention from the fact that the Cold War is over, that there is no East and West anymore. Instead, after 9/11, there is a binarisation of two countries in One over 'ground zero' which we can safely called Usuk[79] , and which represents barbarism on an unimaginable scale. In his speech, Obama sought to address concerns caused by recent revelations of internet surveillance and US drone warfare. He insisted that US surveillance programmes were aimed at 'threats to security, not the communications of ordinary persons'. Of course, he forgot to mention that to get the bad guys you have

[78] Some would argue that the digital human's online activity cannot be qualified as labour. Indeed, adapting a Marxist analysis to the digital/internet industry as a site of exploitation where the owners of capital generate a surplus would be an analogic distortion not dissimilar from the government's understanding of the Web 2.0. Digital slavery is built upon the free cooperation of its victims. It is about liberating users of their freedom by integrating them in systems of automatic and unconscious servitude. Freedom is never gratis, but slavery is. Access to the Web 2.0 is gratis. Draw your own syllogistic conclusion: A digital/internet society *is* a slave society.

[79] In my poems, essays and stories, the US and the UK are two countries incarnated in one biblical Usuk. A descendant of Goliath, Usuk stands alone and against the concept of civilisation and the rest of the countries of the world.

to sift the communications of the good guys for suspicious words, phrases, and clusters that might merit further investigation. It is by targeting the widest possible range of communications and by considering the largest possible number of instances that analysts with the help of computers can establish meaningful patterns and narrow down suspicious results. As I have already mentioned, state-funded snooping is very wide ranging because it has to do with fighting several wars at the same time: War on Terror. War on Crime. War on Drugs. War on antibiotics. War on immigration. War on war itself.

Still, Obama said that the monitoring applied within the narrow limits to do with national security. According to him, it had detected fifty potential threats and saved many lives. In June 2013, Edward Snowden, a former CIA agent, warned the American people about the threat of government snooping. But the data-collection activities of the National Security Agency, America's most secretive institution, is not fundamentally different from that of the men behind WikiLeaks or the more provocative hacking of the group Anonymous, whose members have morphed from cyber vandals who targeted anyone and anything into an organised political movement. Behind the grinning, moustached Guy Fawkes mask of the hacktivist group, numerous persons of radical political affiliations regularly take websites down and steal information to expose secrets. Anonymous has grown into a force to be feared by large corporations and governments. National states and companies are increasingly hiring hackers to try to fix the problems. An elite hacker could be hired many times to defrost the same computer network he had supposedly frozen – machines immediately got corrupted when hired hackers tried to log on to the internal computer network. The only computers safe from hacker attack are those that are not connected to the internet. Yet one day you might go to work only to find people sitting at their desks trying to do their job with pen and paper. It might be the same all over the world. The higher the level of connectivity, the higher the risk of being hacked.

Mass-surveillance programmes carried out on its citizens and alien enemies by democratic states together with governmental calls on technology companies to take down extremist material may have created the conditions which have allowed hacktivism to emerge and thrive in the twenty-first century. Today, both the US and the UK are not *physical* police states but *online* police states. Anonymous is one of many online resistance movements that is fighting against Usuk's occupation of internet space. There are many other hacking collectives active today that endorse libertarian principles; Guardians of Peace immediately comes to mind. Their work is particularly significant because it targets celebrity culture; celebrities being the group most likely to be attacked and destroyed if a libertarian revolution explodes in the twenty-first century. The Sony Hollywood Studio behind the Spider-Man and James Bond films was attacked by the Guardians on 1st December 2014. Even though the Japanese electronics conglomerate Sony seems to attract a lot of hate from the hacking community for their eagerness to sue hackers, the actresses Cameron Diaz and Angelina Jolie, whose private information was stolen, were the intended targets.

Yet the US government claimed that North Korea was behind the attack; apparently, it was motivated by Sony's plans to release a film called *The Interview*, a comedy about two hapless journalists recruited by the CIA to assassinate bogeyman Kim Jong Un, starring Seth Rogen and James Franco. *The Interview* had been set to debut on 25th December 2014, Christmas Day, on thousands of screens. Sony corporation cancelled the theatrical release after the hackers who claimed responsibility for leaking data warned people to stay away from cinemas showing the film, reminding moviegoers of the 9/11 attacks. 'With the Sony collapse America has lost its first cyber-war. This is a very, very dangerous precedent,' tweeted Newt Gingrich, former Republican House of Representatives. Again, why the US government betrays the fact that a cyber-attack on this scale can only be launched by a nation-state? If Sony is a Japanese company, why wouldn't he say Japan has lost its first cyber-war? Gingrich's statement also betrays this perfect lie since it was the movie *War Games* (premiered thirty years ago and starred by Matthew Broderick and Ally Sheedy) that first brought to public attention the possibility of a cyber-attack on the US government. A young computer whizz-kid accidentally connects into a top-secret super-computer which has complete control over the US nuclear arsenal. It challenges him to a game between America and Russia, and he innocently starts the countdown to Global Thermonuclear War. Broderick's character, the dishevelled David, reminds me of many teenagers who spend their days and nights hidden away with their computers.

If Western military intervention gave Islamic State its chance of power, mass-surveillance programmes and internet occupation by the state are giving politically motivated hackers their chance of power. Before 9/11 there were no seriously organised hacking organisations operating in the West. With all the petty crimes hackers committed in those pre-9/11 days, from identity theft to stealing from credit cards and bank accounts, it was a virtual regime that applied secular law and a deviant style of humour which made some steps towards emancipating/enlightening humans. Today a

network of hacktivist decentralised entities operating on ideas rather than people attacks government agencies; media, video, and game corporations; copyright protection organisations, military contractors, and security companies that run prisons are also targeted. So far, governmental efforts at IDing hackers have succeeded in very few occasions as they tend to use primitive and easily identifiable malware during spying operations. However, we have seen a vicious crackdown on the hackers of Anonymous and LulzSec. Like the hacktivist and computer hacker from Chicago, Jeremy Hammond [80], they have found themselves alone in the face of state repression and arrests. If the government and its agencies admitted that all data is accessible in some way or another, this would reduce some of the worst effects of online monitoring, including their levels of stress and our anxiety over their disproportionate overreaction when hackers get caught. Moreover, digital/internet privacy, copyright and encryption are profoundly elitist. They give an unfair advantage to those who can or want to acquire great knowledge and skills. The need to resort to hacking or encryption is not something you might want to do unless you are dealing with a life-and-death situation; and copyright might be only suitable for those who are unfamiliar with the new digital/internet world, where data are copied, combined and metamorphosed beyond recognition at the click of a mouse. New snooping legislation and the prospect of prison is pushing hacker organisations to split into smaller groups. Now the best hackers are aiming for lone-wolf attacks informed by randomness and automatisms. These are the most dangerous type of attack as they cannot be predicted, prevented, or stopped once they are running. Yet the lone-wolf operator is limited in target range and can rarely succeed when attacking critical infrastructures that require 'team' work.

One should not overestimate the role of one single event or one single individual in the great order of things. But it would be a mistake to blame it all on the wickedness of the bogeyman, whether he is the best hacker in the world or the President of the United States. Of course, when Obama withdrew from Iraq and Afghanistan, apparently leaving these regions without US troops/intelligence, he was just responding to a technological change, to a new weapons system that Chris Woods, the historian of America's drones, has called 'the world's first airborne sniper rifle'. Perhaps this is why some people hesitate to call him 'murderer' or 'killer'. When he ordered the execution of bin Laden, for example, he did it with little collateral damage. Very little indeed compared with programmes of targeted killings conducted under previous US President's orders. Think of the massive collateral damage (approx. 100,000 civilian deaths) caused by 4.7m tons of bombs dropped on targets in Cambodia and Lagos between 1965 and 1973 when the US was fighting North Vietnam and the Khmer Rouge. It is estimated that CIA targeted killings with UAVs (Unmanned Aerial Vehicles) in Pakistan, Yemen, and Somalia between 2002 and 2014 have caused 500 civilian deaths with 250 tons of explosives. Inflicting death on the enemy at no human cost to one's side, with minimal collateral damage, and indeed, at a fraction of the cost of a traditional airforce strike: this is a dream come true for warmongering politicians. Yet, the hit lists for targets of drone attacks revealed by Snowden have shattered the illusion of democratic politicians as somehow removed from the daily slaughter that's happening on various battlegrounds across Africa and the Middle East.

2.5 The Data Commons (DC)

The time is ripe for challenging the secret services, not on the grounds of extrajudicial practices such as kidnapping, torture or assassination, but on the basis of their profound misunderstanding and mismanagement of the Data Commons (DC). [81] It is their dogmatic and superstitious defence of secrecy and mystery, along with other quasi-religious attitudes and tenets, such as 'national security' and the 'war on terror', that deplete the data pastures of fertile grass for researches. Prohibiting access to sensitive data or locking up suspected terrorists in Belmarsh/Guantanamo or hiding offending information in data silos are all reactionary moves that tend to inhibit the advancement of science and the progress of civilisation. By removing data labelled classified, sensitive, top-secret, etc., from the DC, these survivors from the pre-digital/internet age, these barbarians of the new information world, are vandalising an important public resource. Moreover, because we are constantly being transformed into data through our constant online querying, we are robbed of a part of ourselves every time data about ourselves is stored in secret or inaccessible locations.

[80] In November 2013, Jeremy Hammond was sentenced to 10 years in prison for stealing internal emails from the global intelligence firm Startfor.

[81] Data Commons is a term coined by Jane Yakowitz to designate anonymised research data 'comprised of the disparate and diffuse collections of data made broadly available to researchers with only minimal barriers to entry. We are all in the data commons; information from tax returns, medical records, and standardized tests seed the pastures. We are protected from embarrassment and misuse by anonymization.' Jane Yakowitz, 'Tragedy of the Data Commons', in *Harvard Journal of Law and Technology*, Volume 25, Number 1, Fall 2011, p. 2-3.

Prohibiting access to secret information today is not dissimilar to the burning of books of old times. BD-driven research requires a total approach to information gathering and sharing. Cancer research, for example, is BD-driven and it has benefitted enormously from institutional openness and data sharing in the last ten years. Cognitive and neurological research, however, is hampered at every stage by access denials and state restrictions. It is sad that WikiLeaks still resorts to primitive practices such as hacking to retrieve information from certain secret silos. Here is a practical exercise of stoicism suitable for democratic governments and large corporations alike: if the administrators of the state and their corporate partners based their expectations of privacy on the worst case scenario – that is, in the case of hacking, that all information is public by default – they would not exude that fearful sense of insecurity, but would be able to plan for cyber attacks in such as way that, when political hacktivists take control of their computer systems, they would not have to panic or react disproportionally.

What the state and its secret services are doing by concealing information is damaging to the national interest. Inhibiting access to certain databases on the grounds of national security is harmful to the whole of the population in ways that a terrorist attack is not. For terrorist attacks affect both the families of the victims and the credibility of the authorities who failed to prevent them, but leave the majority of the population unharmed; whereas the withdrawal of information from the Data Commons (DC) affects society as a whole, as every member is robbed of a piece of itself, and every single individual is prevented from benefitting from the research that could have been effectively carried out with the missing data. On both sides of the Atlantic, high court judges have protested explicitly about the spy agencies use of torture and other legally prohibited practices. Some like judge Bingham in the UK went as far as starting a rebellion which threatened parliamentary democracy with a high-stakes legal confrontation with the executive. [82] If these confrontations between the executive and the judiciary are becoming more and more common in the West as liberal democracy's crisis deepens, it is because they are still the most effective way of asserting the delusion of the division of powers by pretending it is real. [83] The people of US/UK, too, have protested against mass-surveillance by the spy agencies. Yet the main focus of their protests has been privacy rather than the DC – perhaps, most people don't know the DC exists.

2.6 Towards Data Equality (DE) and Total Transparency (TT):

When Alex Younger gave his speech within MI6 headquarters in London on 8th December 2016, his aim was to show that the secret organisation is making an effort to be more transparent. The problem with this move is that it is incremental and teleological, it sets up a trend towards total transparency. A similar move towards transparency was behind the idea of forcing the three UK spy bosses to give evidence before a Parliamentary Commission three years earlier. Echoing his predecessors, Younger mentioned that they had disrupted 12 terrorist plots in Britain since June 2013. He said that MI6 agents are risking their lives daily in Islamic State heartlands to give MI5 and the police vital information to identify and stop threats in the UK and its allies. What he forgot to mention is that success in stopping terrorist attacks in UK's mainland has been TOTAL, whereas success in stopping terror attacks has been NIL.[84] This either means that there have not been any terror/terrorist attempts during that period, or that the secret services have been utterly efficient in stopping them. The latter assertion contradicts a previous statement by the three spy bosses where they insisted that they couldn't stop everything, that somewhere/somehow a terrorist plot would come to fruition.

If the work the agencies do is to be judged for its capacity to lie to the public and against the necessity of protecting the UK against the terrorist threat, surely there can be no need for the secret services if such a threat does not exist. As self-preservation becomes paramount, the temptation for them is to encourage terrorists to commit atrocities, rather than stopping them. Thus counter-terrorism becomes self-generating, a radical monopoly that feeds on itself. [85] The agencies need to reinforce the same threats they combat. By creating new horrors and complicating solutions, the agencies might

[82] See *A v. Secretary of State for the Home Department* [2004] UKHL 56.

[83] The latest of such rebellions *a la* Bingham has happened in the US where federal judge James L. Robart effectively opposed Trump's 90-day ban on entry by citizens of seven majority-Muslim countries (as well as refugee admission for 120 days) with a temporary restraining order.

[84] For the difference between terror and terrorism see Fred Perez, 'Conceptual Distinction between Terror and Terrorism' in *International Journal of Social Science and Humanities Research*, 5:2, April-June 2017, pp. 91-100.

[85] For the practice by Western powers of fabricating terrorism abroad see Jeremy Keenan, *Report on In Amenas: Inquest Cover-up and Western Involvement in Algerian State Crimes* (London: International State Crime Initiative, Queen Mary University of London, 2016). For state-funded terrorism in the pre-digital age, see Daniele Ganser, *NATO's Secret Armies: Operation Gladio and Terrorism in Western Europe* (London & New York: Frank Cass, 2005).

be reinforcing their indispensable role in a psychotic society where the relation between reality and the fantasy is totally asymmetrical – following the pattern of binary oppositions, such as friend/enemy, Christian/Muslim, white/black, native/immigrant, reason/passion, and so forth. But as the moral code becomes a psychotic framework that serves to legitimise social arrangements into which the 'darker' side of these binaries is excluded, someone must be killed to prove the necessity of agencies: the bogeyman.

As the need for total transparency begins to kick in, another temptation for the agencies is to encourage mass migration to the private sector. We've already seen similar public-to-private moves in the police and the military, where ex-army and ex-police personnel take their state-funded training and skills with them to the private sector. [86] I suppose we could make an easy comparison between private security companies and those set up by spooks and spies. But business intelligence companies are an entirely different cattle of fish. Take, for example, Fusion GPS in US and Orbis Business Intelligence in the UK. Both companies provide sophisticated cross-border intelligence research services to VIP customers. Orbis boasts of its 'ability to meld a high-level source network with a sophisticated investigative capability'. [87] Basically, 'a high-level source network' implies a high-level security clearance with access to classified information, state secrets, and other areas of research restricted to the general public.

Powers should be applied in a targeted way and without ethnic or religious discrimination in order to guarantee 'equality of information'. Because psychotic societies are framed by a stringent moral code, they thrive on secrecy. Societies that are xenophobic, sexist, racist, homophobic, and generally intolerant of different lifestyles are also fragile in times of data loss of control. The freer a society is from the grip of the moral code, the easier it is to liberate its data. For example, the fight against 'homophobia' and LGBTI prejudice favours DE (Data Equality) because it is conducive to a situation where data which was previously hidden can be shown. Let us not forget that there are still 73 countries around the world that have criminal laws against sexual activity by lesbian, gay, bisexual, transgender or intersex people. In these countries, information on 'deviant' sexual activity is considered 'sensitive' or 'classified'. Those who are forced to keep their sexuality secret do not find freedom.

To put it simply, achieving DE is not so much a question of challenging established powers like the government and its secret services, or those who pretend to be in control of sensitive information; it is rather a challenge to society as a whole to find nuances in its moral code in order to ensure that this kind of secrecy becomes unnecessary. One note of caution: If the moral code is unnecessarily strict it can be counter-productive and make things worse (say, increasing the friction between nation states to the point of war), but if it is relaxed too far, it may expose institutions and services to un-necessary risks. A society with no moral code, quite simply, disintegrates. Transparency, however, is a necessary risk because, without it, democracy won't be able to survive into the next century. Already, its mask of domination is becoming too thin, being constantly eroded by human rights' violations and back-door fascistic politics.

After Snowden, one would have expected a global crackdown on online spying. But mass-surveillance didn't diminish but increased in proportion to the Big Data metamorphosis of the world. Surveillance tends towards the TOTAL in the sense that every single thing that can be digitalised will be monitored. In the near future, we can expect to see more and more online monitoring by psychotic societies like US/UK, and mass-surveillance programmes much more ambitious than the gigantic Prism and Tempora revealed by Snowden, and its previous incarnation, Echelon. Thanks to the rise of digital/internet technologies, mass-surveillance has become a totalitarian reality. But the gravity towards One, the social psychotic drive towards the TOTAL, hasn't changed since Echelon. We do have total policing, total economy, total privacy encryption, and so forth. What has changed is the volume of data we are dealing with. The total mass of data will double every 18-24 months, according to Moore's Law. [88]

[86] For example, in the UK, G4S, Securitas, Mitie, VSG, OCS, Loomis, Serco and Sodexo Justice Services, are constantly recruiting members of the armed forces and the police to fill job vacancies. These are regulated sector security companies that provide a wide range of services including Security Guarding, Public Space Surveillance, Door Supervision, Cash and Valuables in Transit, Prisons Management and Prisoners Guarding, Close Protection, Manned Guarding, and Key Holding.

[87] See orbisbi.com/our-services/intelligence.

[88] Carver Mead, a professor at the California Institute of Technology, coined the phrase "Moore's Law" to refer to a concept first proposed in 1965 by Gordon Moore, one of the founders of Intel. Moore argued that the number of

To cover up their totalitarian monitoring programmes, democratic states are passing laws that focus on privacy. Privacy is a fundamental human right recognised in the UN Declaration of Human Rights and in many other international and regional treaties. Privacy underpins human dignity and other negative freedoms, such as freedom of speech and association. Many nation states have reacted to the Snowden revelations with legislation that protects this fundamental human right. The Investigatory Powers Act 2016, for example, 'sets out the extent to which certain investigatory powers may be used to interfere with privacy'. In addition, the Act 'imposes certain duties in relation to privacy and contains other protections for privacy'. [89] Apparently, the state has realised that data protection is important and are seriously concerned about privacy online. Their motivation is twofold. On the one hand, they are the custodians of gargantuan databases, so they have to deal with data bases and data models on a daily basis. Databases enable the transformation of random sensor observations into systematic surveillance. This must have given them a self-aggrandising psychotic sensation the idea of how powerful they are. On the other hand, the state subscribes to the old-fashioned idea that the internet is a zone of freedom which is worthwhile preserving. Nostalgic hackers, bloggers and activists would remember how internet used to be seen as a political space, and how it became the favourite revolutionary tool for political movements like the Arab Spring, the Indignados, and Occupy.

3. CONCLUSION

The Snowden revelations brought this age of internet innocence to a sudden and abrupt end. It was as if Eve incarnated in a US traitor had resurfaced from biblical times to haunt our digital/internet paradise and cause a second fall by teasing us with a rotten apple which, of course, we ate. After Snowden, the 'forbidden knowledge' about the global management of data was no longer the exclusive dominium of the state and the big corporations. For the last few years, we have all been collecting, sharing and processing more and more data. Mass-surveillance is, above all, mass-participation in data reproductive sharing. Any information element in the network that allows additional/extra connectivity is desirable. Of course, it is preferable for any forward-looking government to advocate strategies that rely on openness and transparency, such as Free Knowledge, Open Government, Open Data, and Open Code, rather than to encourage and sponsor information restrictions such as copyright and encryption.

PR propaganda strategies, trade and commercial secrets, copyright, state secrets, problems with censorship, legal protection of minors, and data protection are all morally/legally structured and culturally rooted procedures. Yet they can become painful hangovers from a pre-digital/internet information age, where data was expensive and didn't circulate freely or in great quantities in and out of organisations. Unfortunately, in international relations, this backward-looking way of dealing with data may lead to embarrassing situations such as politicians and their foreign counterparts trading information which their secret services have already shared with various partners. To the average internet user, however, these old-fashioned strategies translate more often than not in a 'denial of service'; that is, a temporary or indefinite disruption to a host connected to the internet. What we are witnessing is a loss of control and a change in the behaviour of information that does not fit past procedures and expectations.

To believe in secrecy, one must assume that data can be controlled. Perhaps under the old pre-digital/internet regime of walls, masses, distances, and bodies, data could be controlled. But in the new world of social media and instant networking, people's personal information, ideas, career interests and other forms of data are being shared, copied and edited for free. Here the loss of data control is so evident that any denying of it becomes desperate and ridiculous. And this is what the leaders and rulers of nation states who still insist on privacy have become: desperate and ridiculous. Their anti-immigration and anti-information policies are harming the people more than the worst terrorist attack one could envisioned. Is the Islamic terrorist threat 'real'? Instead of challenging their leaders by subjecting their terror/terrorist fear tactics and assertions to a 'reality check', the people demonstrate in the street and online as if the bogeyman was 'real'. Indeed, no revolution is taken place. Why? Perhaps to get really angry about our leaders' lies and their online surveillance, we would need to go beyond those abstract binary conditions that tap into the moral code of our psychotic society – according to which 'we' are victims and 'they' are perpetrators, 'we' are friends and 'they' are enemies, 'they' represent repression and 'we' represent freedom. The general public tends to confront mass-surveillance by the secret

transistors on a microchip will increase exponentially, typically doubling every 18-24 months. To put it simply, we are producing more data than we can storage.

[89] See *Investigatory Powers Act 2016* (c.25). Part 1 – General Privacy Protections: Overview and General Privacy Duties.

services in this morally coded way. 'Real' mass-surveillance, however, requires more than two opposite actors; in fact, it requires a multitude of languages, machines, and human beings – who can be neither perpetrators nor victims, neither here nor there, neither friends nor enemies.

Instead of defending victims against perpetrators, friends against enemies, and privacy against surveillance, as democratic states are doing, we should fight against the psychotic moral code and its unthinkingness. Us/Them border controls, black/white police cohorts, homophobic social structures, sexism at work and in the home, unequal treatment in health and care systems due to prejudice around obesity, drugs and alcohol, and institutional discrimination in areas such as education – schools and universities where the less-able academically are written off by league tables and systematically bullied by their teachers. Above all, let's not forget that the state itself is a monopoly of force and a grand money-grabbing scheme. From statutory taxation to the bailing out of the banks, the taxpayer fits the bill not only to fund obsolete services and institutions, such as parliament and the secret services, but also pays billions to save the same banks that turn the working poor into wage-slaves with subprime mortgages and other financial scams. Today, data-based credit rating and spy practices are shaped by some combination of friend/enemy oppositional thinking, inconsistent or unreliable sensor/on-the-ground data, the intelligence industry's obsolete practices and rituals, gut-feeling, highly emotional or morally coded responses during, before and after engagement with AI digital assistants, suicidal or catastrophe-driven decision making, and self-serving or career-promoting discretionary choices.

However, neither the banks nor the agencies should be confronted by those morally offended because they have done something wrong. Wrongdoings such as the peddling of dodgy financial products or the use of torture may inflame High Court judges and the general public alike, but they won't reform these services. After all, one could argue that they were doing their jobs. A much more effective strategy for reforming the spy agencies would be to focus on DE (Data Equality) and TT (Total Transparency). Professor Jane Yakowitz is a good starting point. In 'Tragedy of the Data Commons', she argues that Data constitute a common good like the air we breathe and the water we drink, so the reticence of the secret services to share their data with the public is a dangerous act of selfishness which can deplete the social capital of its most important and valuable asset: information. [90]

REFERENCES

[1] @Snowden, Twitter, 9:59pm – 17 November 2016.

[2] A v. Secretary of State for the Home Department [2004] UKHL 56.

[3] Baudrillard, Jean. 'The Roots of Evil' in The Agony of Power (Los Angeles: Semotext (e) Intervention Series, 2011).

[4] Bortolotti, Lisa. Delusions and Other Irrational Beliefs (Oxford: Oxford University Press, 2010).

[5] Bortolotti, Lisa . 'Delusions and the background of rationality' in Mind & Language 20:2, March 2005, pp. 189-208.

[6] Cixous, Hélène. 'Sorties', in New French Feminisms: an Anthology, translated and edited with introductions by Elaine Marks and Isabelle de Courtivron (London: Harvester Press, 1981).

[7] Draft Communications Data Bill (2012).

[8] Draft Investigatory Bill (2015).

[9] Investigatory Powers Act (2016).

[10] Floridi, Luciano. 'A Proxy Culture' in Philosophy & Technology, 28:4, September 2015, pp. 487-490.

[11] Floridi, Luciano. 'Big Data and Their Epistemological Challenge', Philosophy & Technology, 25:4, (2012), pp. 435-437.

[12] Floridi, Luciano. 'Web 2.0 vs. The Semantic Web: A Philosophical Assessment' in Episteme, 6:1, February 2009, pp. 25-37.

[90] See Jane Yakowitz, 'Tragedy of Data Commons', in *Harvard Journal of Law & Technology*, Volume 25, Number 1, Fall 2011.

[13] Ganser, Daniele. NATO's Secret Armies: Operation Gladio and Terrorism in Western Europe (London & New York: Frank Cass, 2005).

[14] Goya, Francisco. Los Caprichos, Hofer Plates (New York: Dover Publications, 1969).

[15] Hill, R.K. 'What an algorithm is' in Philosophy & Technology 29:1, (2016), pp. 35-59.

[16] Sigmund Freud, 'Moses and Monotheism: Three Essays', in The Standard Edition, vol. XXIII (1939).

[17] The Guardian 2, 9 November 2015.

[18] The Independent, 10 December 2015.

[19] Keenan, Jeremy. Report on In Amenas: Inquest Cover-up and Western Involvement in Algerian State Crimes (London: International State Crime Initiative, Queen Mary University of London, 2016).

[20] Kierkegaard, Soren. Repetition and Philosophical Crumbs, trans. M.G. Piety, into & notes by Edward D. Mooney (Oxford: Oxford University Press, 2009).

[21] Korematsu v United States 584 F Supp 1406 (1984).

[22] Nietzsche, Friedrich. 'Preface' in On the Genealogy of Morality (Cambridge: Cambridge University Press, 2010).

[23] Perez, Fred. 'Psychotic Society: An Introduction with a Glossary' in International Journal of social Sciences and Humanities Research, 5:1, pp. 403-418.

[24] Schmitt, Carl. Political Theology: Four Chapters on the Concept of Sovereignty (Chicago & London: University of Chicago Press, 2005).

[25] 'The New MI6: less white and less like Bond' in The Guardian, 3rd March 2017

[26] The Times, 28 October, 2015.

[27] Yakowitz, Jane. 'Tragedy of the Data Commons', in Harvard Journal of Law and Technology, Volume 25, Number 1, Fall 2011, pp. 1-67.