



laetus in praesens

Alternative view of segmented documents via Kairos

8 October 2013 | Draft

Systematic Gerrymandering of Declared Threats and Legality of Response

Opportunistic exceptionalism underlying promulgated rules of governance

-- / --

Introduction

Defining threat, especially from terrorism

Defining legality, especially in response to threat

Defining proof, especially in a context of perceived threat

Enabling gerrymandering through doublespeak in response to threat

Unsuspected "crown jewels" of intelligence community: backdoors to the mind?

Ensuring confidence in democratic supervision

Enabling oversight through simulation of requisite complexity

Transforming from paranoia through metanoia and hyponoia?

Introduction

The crisis of governance and its eroding credibility is highlighted by a confluence of several factors, all variously questionable. These might include: assertions of threat, assertions of proof, assertions of principled response, claims of legality, and assertions regarding adequacy of democratic supervision.

Of particular concern is the manner in which these factors are variously defined and reframed according to unquestionable need. The underhand manner in which this is done bears comparison with the process of gerrymandering characteristic of the manipulation of political constituency boundaries.

The purpose here is to summarize these issues and their interrelationship. It follows from their earlier consideration from other perspectives ("*Big Brother*" *Crying "Wolf"?* *But them "wolves" are a-changin' -- them's becomin' "werewolves"!* 2013; *Vigorous Application of Derivative Thinking to Derivative Problems*, 2013; *Ungovernability of Sustainable Global Democracy?* 2011; *Emergence of a Global Misleadership Council: misleading as vital to governance of the future?* 2007).

Curiously the current period is witness to a situation which those upholding themselves as "good guys" are enabling very "bad things" to happen -- whilst others they have framed as "bad guys" are enabling very "good things" to happen, as upheld by some. The difficulty for the "good guys" in authority is that their power to misrepresent now makes it impossible for them to prove with any credibility that they are themselves not actively engaged in enabling "bad things" to happen.

It is however strange to note how dependent the current complex of conditions is on a definitional process which could readily be challenged as arbitrary. It could be said that the framing of threat, legality and proof effectively hangs in each case by a "conceptual thread". Alternatively, the question could even be asked as to whether the structure of the crisis bears some resemblance to an inverted conceptual pyramid -- one standing precariously on its peak. This vulnerability -- a form of meta-stability -- suggests that the problematic complex is readily susceptible to reframing, whether deliberately or as a consequence of an emerging crisis.

Debate regarding democratic oversight, especially in response to the level of electronic surveillance, has highlighted its inadequacies and the extent to which those defending it are currently part of the problem rather than of the solution. It can therefore be argued that much greater use should be made of tools commensurate with the complexity of the problem, such as simulation, as a means of detecting vulnerabilities and rendering them comprehensible.

There is every justification for the increasing sense of paranoia cultivated by conspiracy theorists. As described in the classic by [Joseph Heller](#): *Just because you're paranoid doesn't mean they aren't after you* (*Catch-22*, 1961). The argument concludes by considering together (in an [annex](#)) the attitudinal options of paranoia in contrast to metanoia and hyponoia. Whilst reference is widely made to the former, the subtler comprehension suggested by metanoia and hyponoia is seldom mentioned but merits attention with respect to consideration of any change of mindset required in order to thrive in present circumstances.

Defining threat, especially from terrorism

Political declarations and related media presentations imply that the definition of terrorism is unquestionable, simple and universally agreed. This is achieved by associating the definition with specific acts involving the loss of life. It is then implied, by extension, that others are suspected of wishing to perpetrate such acts -- therefore to be unquestionably defined as terrorists. The extension goes further with respect to those suspected of aiding and abetting such individuals -- and even further with respect to those inciting to terrorism or sympathetic to the cause of those perpetrating such acts. There is little sense of the variety of forms of terrorism as experienced (*Varieties of Terrorism -- extended to the experience of the terrorized*, 2004).

There is however a great contrast between the ready use of "terrorism" -- to frame a variety of threats and justify a ready-made response -- and the manner in which any definition accords with the evidence relating to that threat. It should not be forgotten the difficulty of [defining "aggression" in international law](#) -- in debates which lasted many years.

Provocatively it has been asked whether God should be considered a terrorist -- given the loss of human life engendered by natural disasters -- so-called "Acts of God" (*Is God a Terrorist? Definitional game-playing by the Coalition of the Willing*, 2004). Any such possibility is complicated by the manner in which deity is invoked in the perpetration of acts of terror on others -- notably through jihad or a crusade.

Uncritical use of "terrorism": It is striking to note the extent to which "terrorism" and "terrorist" are now used uncritically to frame a wide variety of threats. It might then be asked which threats it is no longer considered legitimate to frame in this way. The matter is further complicated by the association, wherever possible, of "Al-Qaida" as being behind the threat -- even though "Al-Qaida" has been recognized as being more a movement of opinion than an organization which could be behind anything (*Questionable "existence" of Al-Qaida*, 2013). The same might be said of "Christianity" which is not an organization -- however many distinct bodies use the term to brand their initiatives.

As some have noted, the pattern bears comparison with [McCarthyism](#) -- the framing offered regarding communism by the [House Un-American Activities Committee](#) during the era of Senator [Joseph McCarthy](#). It also merits comparison with analogous framings made by the UssR and China during the Cold War. Historically it bears comparison with the [witch hunts](#) of both Catholic and Protestant faiths.

The current simplistic approach can be further challenged with respect to:

- efforts to frame "extremism" in general as characteristic of "terrorism" (*Norms in the Global Struggle against Extremism: "rooting for" normalization vs. "rooting out" extremism?* 2005)
- recognition of how iconic figures of independence movements may well have been labelled "terrorist" by the regime to which they offered resistance (eg George Washington, Nelson Mandela, Jomo Kenyatta). The phenomenon is especially striking in the case of Israel for which those termed "terrorists" included David Ben-Gurion, Menachem Begin, Yitzhak Shamir and later, Ariel Sharon (Ted Pike, *Israel: founded on terror*, *National Prayer Network*, 25 March 2008). This poses the question of "good terrorists" versus "bad regimes"
- the degree to which those accused of terrorism may be incarcerated without charge for extended periods of time -- supposedly contrary to principles of justice
- the extent to which such oversimplification stands unchallenged by those in authority, especially when it can be used as a form of "blank cheque" to elicit further funding for security to the benefit of the [military-industrial complex](#)
- terrorists as those others who disrupt the status quo and business as usual however problematic these may be perceived to be

Necessary quest for "bad guys": The justification of invasive electronic surveillance as being a legitimate quest for the "bad guys" (specifically "terrorists" and "pedophiles") is proving dubious when it has clearly proven to be inadequate to detect the "bad guys" involved in other questionable activities (to the point of going unreported). Most significant in this respect, post 9/11, has been the seeming total inability to detect the "bad guys" who enabled the financial crisis from which so many have suffered -- whether to the point of loss of livelihood, or even to loss of life.

Why has such sophisticated surveillance proven inadequate to that end when it has been employed -- controversially -- to enable economic espionage as in the case of Brazil (Anthony Boadle, *NSA spying on Petrobras, if proven, is industrial espionage Reuters*, 9 September 2013). Again, why the controversy regarding electronic surveillance of the UN (*Alleged Breach of UN Treaty Obligations by US: press coverage and commentary following WikiLeaks cable dissemination*, 2010)?

Should extreme financial risk-taking be recognized as a form of "terrorism" -- given the manner in which it has endangered the security of whole countries (*Extreme Financial Risk-taking as Extremism -- subject to anti-terrorism legislation?* 2009)? If not, why not? Is it reframed as "good for business"?

Unsubstantiated assertions of threat: The assertion of threat is readily made on the basis of secret knowledge -- with the implication that every confidence should be had in that assessment, despite indications to the contrary. This is clearly of the greatest convenience to those in authority, as discussed separately (*Promoting a Singular Global Threat -- Terrorism: strategy of choice for world governance*, 2002; *Spin and Counter-spin: Governance through Terrorism*, 2002).

Mention of "terrorism" is then readily used as a trump card, justifying the setting aside of all other considerations -- and justifying every expenditure on any response.

There is the further possibility that any questioning of that assessment should itself be framed as a threat (and potentially an even more dangerous one). This has been strikingly illustrated in a related strategic domain namely the disruption of consensus by science and critical discourse -- and measures taken to constrain it.

Unrecognized threats: It is appropriate to ask whether there other current initiatives, which the future may well frame as "crimes

against humanity". These could merit recognition as "terrorism" -- if only in the terror they may engender for future generations through their consequences. What might those be and why is no consideration given to them, or to that possibility?

The question is pertinent in the light of two new projects, that of the [Cambridge Centre for Risk Studies](#) and that of the formation of the [Centre for Study of Existential Risk](#) by [Martin Rees](#) (*We Are In Denial About Catastrophic Risks*, *Edge*, 16 January 2013). The question with regard to such initiatives is not what they choose to focus on but rather what they exclude from consideration and how that is to be recognized -- together with its systemic implications.

Such concerns have been discussed separately (*Lipoproblems: Developing a Strategy Omitting a Key Problem -- the systemic challenge of climate change and resource issues*, 2009; *Scientific Gerrymandering of Boundaries of Overpopulation Debate: Review of The Royal Society report -- People and the Planet*, 2012). Of particular interest at the time of writing are the arguments in the debate regarding the "shutdown" of the US Federal Government -- both positions being framed as a form of strategic blackmail.

By contrast, the question of deliberate or inadvertent omission of what is framed as a threat was central to the problem selection and profiling of the [World Problems Project](#) -- as part of the *Encyclopedia of World Problems and Human Potential*. The question is who defines what is a threat and who has the authority to acknowledge that it is a threat -- and how does this relate to issue of collective intelligence in the detection of problems and the articulation of remedies (*Enabling Collective Intelligence in Response to Emergencies*, 2010).

Of particular interest is the framing of "terrorism" in relation to national security -- even to Homeland Security in the USA. There is no sense of "global security" as might be implied by resource overshoot -- from a larger systemic perspective.

Defining legality, especially in response to threat

Any challenge to the high level of invasive electronic surveillance is met with the response that the initiatives were all undertaken within the law and that their legality is carefully ensured. This claim is made despite the level of secrecy with which those initiatives may have been instigated and the unchallenged manner of their supervision. In the USA this is exemplified by the manner in which the legality is established secretly through authorization by [FISA](#).

Plea of Legality: Through the recent debate on the invasive surveillance and the degree of collaboration between partner countries, great emphasis has now been placed on its legality.

It is therefore interesting to consider the Plea of Legality from a legal perspective. The problematic history of this plea was made evident in relation to the Nazi justice system and the [Nuremberg Trials](#) -- with the latter framed by the [Nuremberg Principles](#) in defining a [war crime](#). The same could be said of the [Apartheid Regime of South Africa](#). Within both contexts very careful attention was made to the legality of actions taken and their authorization by due judicial process. This could also be said to be true of the UssR and China, each with their particular judicial system.

It has been from another context -- another jurisdiction -- that the "legality" of initiatives within any of those frameworks has been claimed to be "illegitimate". The jurisdiction within which that claim is made is held to be "universal", and of a higher order of morality, as defined internationally through a pattern of international treaties. This is claimed to be the rule of law superseding that of such regimes. This precedence is claimed whether or not a given country accedes to relevant treaties or fails to do so -- as in the case of the USA with respect to the jurisdiction of the [International Criminal Court](#).

At this point in time, three groups are making very significant use of the Plea of Legality -- if only implicitly, since they are seldom indicted for their actions:

- those responsible for instigating, financing and sustaining an unsuspected level of electronic surveillance
- those in the financial community (especially bankers) who variously enabled the high level of risk-taking which resulted in the global financial crisis. Suggestion for analogous trials have been variously made (Dave Hodges, *Nuremberg Trials for the Banksters*, 9 January 2013; *A Nuremberg Trial for Speculators is Necessary: an interview with Jean Ziegler*, 20 January 2011; *"Economic Holocaust" and the Nuremberg Trials for Bankers*, *Risk Latte*, 14 February 2009)
- those involved in instigating levels of enhanced interrogation of prisoners which are difficult to dissociate from torture (Larry Siems, *The Torture Report: what the documents say about America's post-9/11 torture program*, 2012; [Philippe Sands](#), *Lawless World: America and the Making and Breaking of Global Rules*, 2005; *Torture Team: Rumsfeld's Memo and the Betrayal of American Values*, 2008). As in the case of the Nazi regime, this might extend to those complicit in that process, as argued by Roy Eidelson and Stephen Soldz (*Hawaiian Mind Games: APA fiddles while psychology burns*, *Psychology Today*, 5 August 2013) with regard to the central role psychologists play in US government torture and abuse of national security detainees, with the apparent protection of the [American Psychological Association](#).

It is unlikely that the most responsible figures in any of these cases will be prosecuted for any form of misdemeanor.

Of interest is then the basis on which the Plea of Legality was rejected in the Nuremberg Trials. Clearly this was achieved by rejecting the legality of the Nazi Regime, if only with respect to selected instances, however assiduously it operated according to its own legal principles. The framing which superseded that legal regime was that established by the United Nations following World War II. This framing enabled the Nuremberg Trials and established their legitimacy. Would it have enabled similar trials with respect to the UssR -- had it been defeated in the course of the Cold War?

How is a "war crime" to be distinguished from a "crime against humanity"?

Retroactive prosecution: It is especially interesting that within any existing regime it is typically inadmissible to prosecute individuals retroactively in the light of legislation newly elaborated, namely on the basis of retroactive law ([ex post facto law](#)). This principle does

not apply with regard to the treatment of those whose Plea of Legality relates to a regime whose principles have been deprecated -- effectively by some form of military defeat. The continuing legal proceedings -- against those whose "legal" activities decades ago are now deprecated -- offer cases for reflection (as in Argentina and Chile). Of interest is the sensitivity of George W Bush to this possibility (Paul Craig Roberts, *Bush Seeks Retroactive Laws to Protect Himself from War Crimes Prosecution*, *Information Clearing House*, 29 August 2006).

Questions could of course be asked with regard to the nature of transactions within a deprecated regime which were honoured (and considered "honourable") subsequent to that defeat. Many transactions within that regime would of course be considered legitimate thereafter.

Plea of Obedience to Orders: This plea was presented in the notorious case of [Adolf Eichmann](#). It was rejected. It is interesting, from a legal perspective, to compare that case with that of [Kofi Annan](#), during the period when he was directly responsible for UN peacekeeping operations in arenas which developed into notorious forms of massacre. It could be argued that in both cases there was a similar tragic failure to disobey orders in the light of higher moral principles (*Perplexing Symmetries in Obedience to Orders: equivalencies in the moral abdication of Adolf Eichmann and Kofi Annan?* 1998).

Plea of Immunity from Prosecution: This plea is widely used by those who have held high office which automatically provides for such immunity -- irrespective of the highly dubious acts for which responsibility there is thereby avoided. It is noteworthy that this plea is rejected in the case of leaders of developing countries, although the African Union is arguing otherwise (*African Union says ICC should not prosecute sitting leaders*, *The Guardian*, 12 October 2013). It is however considered unchallengeable in the case of leaders of industrialized countries (whether or not they have acceded to the International Criminal Court), as argued by Glen Ford (*If Charles Taylor is a War Criminal, then so are Obama, Bush and Clinton*, 2013), with respect to the instigation, encouragement and collaboration in the worst genocide since World War Two.

Plea of Diminished Responsibility: It could be variously argued that there are conditions under which diminished responsibility can be claimed, especially in battlefield situations. This applies notably with respect to "[collateral damage](#)" occasioned during combat missions. Careful argument could then reframe a variety of abuses resulting in loss of life. Combat stress could be used to excuse some such consequences.

A form of diminished responsibility could be claimed with respect to the sale of firearms and other weaponry. A legal defence that is vigorously protected in the US is that of the [Second Amendment to the Constitution](#) relating to the sale of firearms. In extending the Pax Americana and the US concept of democracy, this principle could be understood as extended to any responsibility for the use of weapons elsewhere (*Arming Civil Society Worldwide: getting democracy to work in the emergent American Empire?* 2001). The relevant slogan is of course: *Guns don't kill people, people do*. Missing is the extension of this logic to weapons of mass destruction, including the chemical weapons so extensively deplored in Syria. Curiously no response corresponding to their destruction in Syria has been envisaged with respect to other countries where guns continue to be responsible for a far greater number of deaths.

The sense of diminished responsibility also applies to the manufacture and sale of such weapons and their munitions -- irrespective of their destructive potential (but with the noted exception of Iran and North Korea). No effort is made to highlight by whom the weapons used in major disasters were supplied and they incur no responsibility in the matter, as separately discussed (*Identification of Bullets: human right and human responsibility?* 2009).

Plea of Ignorance: Although ignorance is not accepted as a valid plea before a court of law (*Ignorantia juris non excusat*), it could be argued that ignorance of higher principles, possibly as enshrined in international treaties, is a valid plea -- irrespective of whether it is rejected. Especially intriguing is formulation of the plea in the light of a claimed failure of memory -- necessarily to be construed as ignorance. This was remarkably exemplified by the case of [Ernest Walter Saunders](#), best known as one of the "Guinness Four", a group of businessmen who attempted fraudulently to manipulate the share price of the Guinness company. He was sentenced to five years' imprisonment, but released after 10 months as he was believed to be suffering from [Alzheimer's disease](#) -- which is incurable. He subsequently made a full recovery.

Plea of Precedence of Alternative Legal Regimes: The question of legality is considerably complicated by [legal pluralism](#), namely the co-existence in the same area of different jurisdictions in terms of which legality may be claimed. Obvious examples include:

- religious law, as exemplified by the precedence sought for the [Canon law](#) of Catholicism, the [Halakha](#) of Judaism or the [Sharia](#) of Islam
- military law, as defined by systems of [military justice](#), which is especially significant when there is any conflict between occupying forces and the legal system in place -- notably widely publicized by incidents of rape (*Incidents Involving US Military in Okinawa, Close the Base*; Rick Mercier, *Way Off Base: the shameful history of military rape in Okinawa, On the Issues*, 1997)
- ad hoc justice as meted out by so-called [kangaroo courts](#) or [drumhead court-martials](#) in which the principles of law and justice may be disregarded or perverted
- tribal law, most notably in the form of the indigenous law of peoples whose lands have been occupied by colonization. This can be fruitfully discussed in terms of the conflict between "law" and "lore" (*Law and Order vs. Lore and Orders? Imagining otherwise the forceful engagement of singularity with plurality*, 2013)

Consideration of legal pluralism can be fruitfully considered in relation to the historical trial of Jesus under Roman Law and in relation to that of Judaism. Provocatively it could then be asked how those of that time, held to be breaking the law, would now be processed -- whether or not they appealed to a higher morality (*Would Jesus Now be Prosecuted by US? As a law-breaker -- like Manning, Assange and Snowden -- Yes we can!* 2013)

Emergence of a new global legal regime: In this light, it could then be asked whether a legal regime might emerge (or be recognized) which would supersede that under which a Plea of Legality is currently made with respect to electronic surveillance, enhanced

interrogation, or dangerous risk-taking. Is there the possibility that the Plea of Legality would then be rejected in a similar manner? The point is usefully emphasized by the continuing threat to the prosecution of [Henry Kissinger](#) for actions legally undertaken in the 1970s, as articulated by [Christopher Hitchens](#) (*The Case Against Henry Kissinger: the making of a war criminal*, *Harpers Magazine*, March 2001; *The Trial of Henry Kissinger*, 2001)

Especially interesting would be the possibility of claims of a higher order of morality than that embodied in current international law -- which readily ignores the implications of the final article in the [Universal Declaration of Human Rights](#):

Article 30: Nothing in this Declaration may be interpreted as implying for any State, group or person any right to engage in any activity or to perform any act aimed at the destruction of any of the rights and freedoms set forth herein.

Such issues raise the question of how to distinguish between the initiative of authorities in "taking the gloves off" in response to threat and the action of others acting beyond the law (according to a higher morality) and being condemned as terrorists for doing so (E. L. Gaston, *Taking the Gloves off of Homeland Security: Rethinking the Federalism Framework for Responding to Domestic Emergencies*)

Imposition of an extraterrestrial legal regime: Whilst the argument might be considered hypothetical, the manner in which colonial powers have elaborated legal regimes to supercede those operating in the countries they occupied, suggests consideration of the arrival of "extraterrestrials" with their own legal principles. These might well be (forcefully) implemented to supercede those established by humanity -- especially if their sophistication was as great as that claimed by colonial powers for their own relative to the primitive legal provisions of indigenous peoples.

Especially interesting is the possibility that legal regime of extraterrestrials might combine both a higher morality and an extreme sensitivity to the principles effectively enacted by human behaviour (*Writing Guidelines for Future Occupation of Earth by Extraterrestrials: Be done by as you did ?* 2010). The possibility may also be explored by comparing the strong resolution recently formulated by the UN Security Council with respect to Syria with one which might be formulated by an Interplanetary Security Council with respect to the Planet Earth (*Global Security from an Interplanetary Perspective: Interplanetary Security Council -- Resolution on Planet Earth*, 2013).

Defining proof, especially in a context of perceived threat

Of great interest in this period is the definition of proof. This is considerably complicated by the extent to which parties in any debate explicitly accuse those they oppose of lying. At the time of writing this especially evident with respect to the debate regarding [Obamacare](#) in relation to the [US national debt](#). There are numerous web references to such "lies".

Immediately prior to the urgency of the current debate has been the case of chemical weapons in Syria, and the various explicit claims that different parties were lying, as discussed separately (*Truth Test on Syria: Religious oath -- Polygraph -- Ouija board?* 2013). Of obvious relevance is the extent to which the appreciation of what constitutes strong evidence is politicized (*Politicization of Evidence in the Plastic Turkey Era: al-Qaida, Saddam, Assassination and the Hijab*, 2003).

This intense debate has been held against a background of concern regarding the development of nuclear weapons capacity by Iran and the requirement for "concrete proof" that it was not doing so. This debate continues to be complicated by the questionable positions of other parties in relation to the issue (*10 Unanswered Questions on Iran and Israel*, 2012).

The issue of "concrete proof" can of course be placed in a more general context (*10 Demands for Concrete Proof by We the Peoples of the World*, 2012)

The issue is further complicated by the extent to which "evidence" and "proof" can be variously manipulated and fabricated. Evidence may be planted. Targets may be "framed" thereby. On a larger scale this is evident in [false flag operations](#) which provide tangible "proof" -- readily framed as unquestionable. Such possibilities are extensively explored by conspiracy theorists.

As noted above, the difficulty in this context for the "good guys" in authority is that their power to misrepresent now makes it impossible for them to prove with any credibility that they are themselves not actively engaged in enabling "bad things" to happen. The difficulty is compounded by that of [proving a negative](#).

Enabling gerrymandering through doublespeak in response to threat

The current period offers every opportunity to observe the manner in which issues are reframed, shuffled and rendered questionable. This has been well documented with respect to the "merchants of doubt" within the scientific community by [Naomi Oreskes](#) and [Erik M. Conway](#) (*Merchants of Doubt: how a handful of scientists obscured the truth on Issues from tobacco smoke to global warming*, 2010). It is most notably in relation to climate change (Michael E. Mann, *The Hockey Stick and the Climate Wars: dispatches from the front lines*, 2012)

The process has become even more evident in the debate regarding the disclosures of the level of internet surveillance. The quality of bluster and obfuscation is remarkably evident in BBC debates with [Baroness Neville-Jones](#) (Chairman of the British [Joint Intelligence Committee](#), Minister of State for Security and Counter Terrorism) -- on separate occasions with [George Galloway](#) (*Syria and chemical weapons: Galloway and Neville-Jones*, *BBC News*, 12 September 2013) and with [Glenn Greenwald](#) (*Pauline Neville Jones in debate with Glenn Greenwald*, *BBC Newsnight*, 3 October 2013).

The "sleight of hand" employed in discussion of such matters is striking. It is reminiscent of traditional fair ground confidence trickery and its adaptation to modern marketing through the careful use of distraction -- ensuring a focus on the right hand to reduce awareness

of the action of the left hand. The point is exemplified by the memo of government special advisor (and spin doctor) **Jo Moore** to Tony Blair regarding 9/11 (Andrew Sparrow, *Sept 11: "a good day to bury bad news"*, *The Telegraph*, 10 October 2001).

As an extension of political gerrymandering, the process may be generalized (*Conceptual gerrymandering and definitional game-playing*, 2002; *Exclusivism: gerrymandering, question avoidance, denial*, 2013). It can be understood as combined with doublespeak, as separately argued (*Enabling Suffering through Doublespeak and Doublethink: Indifference to poverty and retributive justice as case studies*, 2013):

- Enabling suffering through religious doublespeak
- Enabling suffering through legal doublespeak
- Enabling suffering through political doublespeak: Iraq vs. Syria

Unsuspected "crown jewels" of intelligence community: backdoors to the mind?

Crown jewels: In relation to the widely publicized disclosures of Edward Snowden regarding electronic surveillance, various reports indicated that these did **not** include the "crown jewels" (Barbara Starr, *Snowden did not access "crown jewels" of NSA intel, official says*, *CNN*, 23 July 2013; *Did Snowden steal NSA crown jewels? We don't know*, *Daily Kos*, 30 August, 2013). The ongoing damage assessment purportedly indicates he did not gain access to what is called ECI or "extremely compartmentalized information".

In commenting on that report, the phrase that has been used is "deep dark secrets of the NSA" (*Intelligence Officials Can't Keep Story Straight: Snowden both did and did not get key NSA secrets*, *TechDirt*, 26 July 2013; Ta Kung Pao, *PRISM Program: How Many More Hidden Secrets? Watching America*, 27 July 2013). As noted by the latter:

In other words, although Snowden leaking the U.S. PRISM program shocked the world, this was just the tip of the iceberg -- nobody knows just how many dirty secrets Washington really has.... But this is far from everything that the United States is monitoring. According to media that understand the situation, besides the PRISM project, the United States also has at least three other secret surveillance projects. Stellar Wind, a surveillance program that was never made public, is split into four projects: PRISM, "TRUNK," "DOCK" and "NUCLEAR." As for what state secrets these code names for strange projects contain, the outside world does not know.

The disclosures already made have been conveniently presented in summary form by *Al Jazeera* (*Timeline of Edward Snowden's revelations*, September 2013). Given the surprising nature and extent of these, it is appropriate to speculate on the nature of the "crown jewels" which remain concealed. For this purpose it can be usefully assumed that what has not been revealed is even more surprising and unexpected.

In engaging in such an exploration, it is appropriate to recall the level and nature of past denial regarding electronic surveillance -- **prior** to the disclosures. At present this is now carefully reframed by those complicit in the denial in terms such as "everyone knew it was going on" -- although no one chose to admit it. However many had little wish to suspect extensive surveillance and the vulnerability of their communications -- and framed any suggestions to that effect as cynicism and/or paranoia. This suggests a need to explore the nature of "crown jewels" with a degree of speculative freedom, which (methodologically) should necessarily evoke similar comments -- despite the implication as to their surprising nature.

The approach taken here is to use many current features of computer and telecommunications use as a template -- potentially a richly structured metaphor through which the nature of the "crown jewels" might be recognized, as they might apply to cognitive processes rather than to electronic communications.

Computer front-ends and backdoors -- and their cognitive analogues: It has been reasonably clear that [Internet Service Providers](#) (ISPs) have long been legally required to hold data regarding the communications of internet users -- for the possible perusal by security services when appropriately authorized (most notably in relation to threats of terrorism). It has been less clear that corporations deriving income from [web search engine](#) requests were offering (or required to offer) a degree of privileged access under some commercial arrangement to security services (and possibly also to other's on a commercial basis). There was some suspicion that such clients constituted a significant source of income for the corporations in question -- contributing to their remarkably rapid development.

The biggest surprise has come from the previously unacknowledged level of complicity of corporations offering web search facilities with the security services, primarily in the USA. Firstly denied by those corporations, it is now recognized that they have been subject to a secret legal obligation to provide search engine requests systematically to the security services. This has also become apparent to a degree in the case of those providing e-mail facilities, which were supposedly a confidential service to clients. The corporations may well have been financially compensated for this access.

It is then appropriate to describe corporations in this position as acting as a "[front-end](#)" for the security services -- effectively putting a "friendly face" on their exigencies, and misleading their clients in that regard. The approach is somewhat reminiscent to the use of "[front organizations](#)" acting for another body without their actions being attributed to that other body.

The complicity of corporations has however extended further to include those providing computer operating systems and security facilities. In such cases secretive arrangements have been made requiring that "[backdoors](#)" be inserted into coding specifically designed to prevent intrusion into such systems. These backdoors allow the security services to bypass such protective features in order to penetrate the computers of individuals (or groups) connected to the internet.

In the quest for "crown jewels", one intriguing possibility is that widely appreciated knowledge systems are designed and promoted by authorities such as to have analogous (secret) features -- known only to the few, and readily denied by those aware of their existence:

- **Cognitive front-ends?:** What form might such a "front-end" take? The analogy suggests that particular authorities, disciplines and movements of opinion would enable people to be "drawn into" the domain of influence of modes of knowledge whose existence is not suspected. This could be with, or without, the complicity of the (friendly) front-ends. This accords with the suspicions which some bodies of knowledge arouse from other perspectives -- whether rightly or wrongly .
- **Cognitive backdoors?:** This would imply that some modes of knowledge have built into them, deliberately or inadvertently, means through which that mode of awareness can be manipulated. Again this accords with some suspicions aroused by some bodies of knowledge from other perspectives -- whether rightly or wrongly

Other technomimetic possibilities

- **Computer viruses and malware -- and their cognitive analogues:** There is ready recognition of the possibility of mental viruses, possibly understood as memetic viruses (*Memetic and Information Diseases in a Knowledge Society: speculations towards the development of cures and preventive measures*, 2008). These could well be designed to be triggered under particular future conditions:
 - **Cognitive malware as an indication of an alternative perspective?** The promotion of the arguments of any opposing movement may be framed in this way -- as an "infection" or "contamination" of public opinion. The process is partially associated with that of "viral marketing". The concern is how to recognize the existence of such malware, especially since it may simply be the (innocent) characteristic of another perspective -- however harmful that be be framed to be with respect to preferred cognitive modalities.
 - **Memetic warfare:** More intriguing is the possibility of designing ever more sophisticated forms of malware as part of a process of memetic warfare -- analogous to what is already recognized as the possibilities of cyberwarfare (*Missiles, Missives, Missions and Memetic Warfare: navigation of strategic interfaces in multidimensional knowledge space*, 2001; *Cognitive Ballistics vs. Derivative Correlation in Memetic Warfare: suicide bombing as a weapon of mass distraction?* 2009)
- **Infected software upgrades -- and their cognitive analogues:** Every computer user is aware of the extent to which software may be automatically "upgraded", with or without explicit approval. Arguments are frequently presented for "new thinking" and revision of "incorrect thinking" of the past -- analogous to "bug fixes":
 - **Cognitive engagement with "programs":** The very language of "program" now permeates use of the media, conference organization, training courses, and the like. Interaction with media in any form implies conscious or unconscious cognitive entrainment by "programs". It is not difficult to argue that people are effectively programmed thereby. People may acquire new programs -- notably by downloading "apps" or upgrades. The question is in what way such programs could be "infected" by the insertion of "backdoors" -- as is so evident with the inadvertent infection by viruses. The argument has been partially developed separately (*Internet Nescience? Self-referential upgrading of obsolete Internet conference processes inhibiting emergence of integrative knowledge*, 2013)
 - **Cognitive analogues of infected malware removers:** There is widespread understanding of the value and operation of firewalls, malware removers, and registry cleaners. There is every possibility that some of these applications may themselves enable creation of backdoors. There is therefore a case for imaginative exploration of how cognitive analogues might be designed into programs upheld as someform of cognitive protection or repair.
- **Censorship and filter bubbles -- and their cognitive analogues:** Issues of internet censorship are widely publicized, as with awareness of the technical possibilities of doing so, especially for a given country or institutional complex. They may well be understood as designed to protect certain cognitive modalities, especially through propaganda in support of particular political agendas. Further possibilities could be envisaged:
 - **Engendering ignorance or bias:** This is most readily foreseen in terms of the process of **dumbing down**, namely the deliberate diminishment of the intellectual level of the content of schooling and education, of literature and cinema, and of news and culture. The possibilities are especially evident in the manipulation of algorithms of search engine (acting as front-ends for the intelligence community), most notably through the creation of **filter bubbles** (*Filter bubbles in internet search engines*, *BBC Newsnight*, 22 June 2011; Doug Gross, *What the Internet is hiding from you*, *CNN*, 19 May 2011)
- **Strategic denial of service -- and its cognitive analogues:** As an extension of the process of censorship, analogues to **denial-of-service attacks** can be readily imagined, possibly of an active form rather than a simply passive one characteristic of surveillance:
 - **Cognitive attacks?**
 - **Credibility attacks:** credit card / passwords
 - **Framing:** identity theft / planting evidence / fitted up

Every such possibility can of course be denied, or framed as of marginal significance, with no possibility whatsoever of proving that none has been activated or is being explored.

It is worth asking what strategic options will become open to the intelligence community programs once everything is known to them -- total information awareness -- and that they are legally empowered to act on that knowledge. However this is achieved to a "high level of confidence", the condition is reminiscent of the naive 19th century belief in a mechanistic universe in which the "capacity to take apart" through analysis provided adequate explanation to predict the future. This provided no demonstratable "capacity to put together" creatively -- and now only enable the targetted "assassination" of those who might interfere with the emergence of "more of the same". The confidence of such confidence is of course completely called into question by "black swans" as articulated by arguments of Nassim Nicholas Taleb (*The Black Swan: the impact of the highly improbable*, 2007; *Antifragile: things that gain from disorder*, 2012) and Pablo Triana (*Lecturing Birds on Flying: can mathematical theories destroy the financial markets?* 2009)

Ensuring confidence in democratic supervision

The argument here is partially extracted from an earlier discussion (*Ambiguity of "democratic oversight": institutionalisation of negligence?* 2013).

Oversight: At the time of writing there is considerable debate about the existence and adequacy of "democratic oversight" of the NSA/PRISM surveillance program, notably as articulated by Glenn Greenwald (*Glenn Greenwald Mocks Robust Oversight' of NSA Spying*, *Infowars.com*, 4 August 2013).

A number of bodies have long been concerned with the process more generally -- whether termed "[congressional oversight](#)" or "parliamentary oversight". Serious concerns have been expressed regarding the adequacy of oversight -- expressed over decades. The bodies include the [Parliamentary Oversight Global Task Force](#) and the [Inter-Parliamentary Union](#). There are many documents relating to the process (*Parliamentary Oversight of Intelligence services*, DCAF, 2006; *Oversight and Guidance: the relevance of parliamentary oversight for the security sector*, DCAF; *Tools for Parliamentary Oversight: a comparative study of 88 national parliaments*, IPU, 2007). Presumably their relevance to the secretive issues of electronic surveillance have yet to be fully clarified in the light of the recent disclosures.

In the secretive context of NSA/PRISM, access by duly elected representatives to information enabling appropriate democratic oversight is itself a challenge, as recently highlighted (Glenn Greenwald, *Members of Congress denied access to basic information about NSA*, *The Guardian*, 4 August 2013; Scott Lemieux, *4 Ways the Government Keeps You In the Dark About What It's Doing*, *AlterNet*, 9 August 2013).

Ambiguity: Irrespective of the degree of "access" and the quantity of information provided -- perhaps deliberately to the point of overloading any such "oversight" process -- there is the question of how effectively the process can be performed (beyond the need to make that claim for public relations purposes). **There is an irony of the highest order in the ambiguity of "oversight" -- indicative as the term also is of negligence, blindspots, and forgetfulness** -- all suggestive of the "intelligence failure" originally associated with 9/11. In that sense "democratic oversight" could be understood cynically as a total pretence -- the institutionalisation of systemic negligence.

In the light of progress in this matter over the years, previous recommendations to strengthen "democratic oversight" merit consideration in this cynical light, as with those of [Robert M. Gates](#) (*Strengthening Congressional Oversight of Intelligence*, *National Security Law Report*, 1993). Gates was [Director of Central Intelligence](#) (head of the CIA) from 1991 to 1993 and US Secretary of Defense from 2006 to 2011, succeeding Donald Rumsfeld. Controversy surrounds [his involvement in the Iran-Contra scandal](#).

Quality of oversight: Expressed otherwise, **would anyone want to fly in an airplane subject to security and safety checks of a quality equivalent to that currently advocated for "democratic oversight"?** This can be extended into the more complex example offered by a system of air traffic control. What standards of "oversight" would be applied to ensure collision avoidance on flight paths over a region?

How does the quality of that oversight compare with the industry [Six Sigma](#) standard? It would be normal to expect NSA supercomputers to be operating according to that standard.

A Six Sigma process is one in which 99.99966% of the products manufactured are statistically expected to be free of defects (3.4 defects per million). As noted by *Wikipedia* with respect to manufacturing processes, Six Sigma:

... uses a set of quality management methods, including statistical methods, and creates a special infrastructure of people within the organization ("Champions", "Black Belts", "Green Belts", "Yellow Belts", etc.) who are experts in the methods. Each Six Sigma project carried out within an organization follows a defined sequence of steps and has quantified value targets, for example; process cycle time reduction, customer satisfaction, reduction in pollution, cost reduction and/or profit increase.

Is there a case for envisaging [Six Sigma "Black Belt" capacity](#) in the democratic oversight process (*Six Sigma Master Black Belt Body of Knowledge*, 2013)? What might then be the "quantified value targets"? Curiously SIGMA is also the abbreviation for the [Support for Improvement in Governance and Management](#) -- a joint initiative of the European Union (EU) and the Organisation for Economic Co-operation and Development (OECD).

Commensurate sophistication and requisite complexity? By contrast, **does the quality of oversight correspond in practice to that employed in target acquisition by drones in remote areas** -- namely tolerance of any unfortunate killing of innocents as being statistically acceptable? This is an issue highlighted by [Bradley Manning](#) in releasing a video via Wikileaks (*Collateral murder in Iraq by US helicopter*).

The challenge has been recognized in the UK (Conal Urquhart, *GCHQ and security services 'need parliamentary oversight'*, *The Guardian*, 22 June 2013). It is further illustrated there at the time of writing, in another arena for which a system for "democratic oversight" is purportedly in place (Rob Evans, *Serious Fraud Office admits losing thousands of documents linked to BAE Anti-fraud unit*, *The Guardian*, 8 August 2013). Are there embarrassing comparisons to be made with the leaking of documents by Snowden? Although a procedural review is envisaged in that case, are such reviews merely exercises in dangerous tokenism -- reflecting an outmoded mentality -- in the absence of adequate simulation to detect potential "holes"?

Similarly, in the course of a major press conference, Barack Obama indicated as a confidence-building initiative that he would work with Congress to reform NSA's FISA court and Patriot Act (Paul Lewis and Spencer Ackerman, *Obama touts NSA surveillance reforms to quell growing unease over programs*, *The Guardian*, 9 August 2013; *Barack Obama pledges greater surveillance transparency*, *BBC*

News, 9 August 2013). However he made clear that mass surveillance would continue. Using the same test, who would have the confidence to fly in an airplane dependent on initiatives of that quality? Who would fly in a plane whose safety was pledged by a politician? The parallel with Obama's health care proposals, in terms of the quality of safety nets, merits reflection.

Enabling oversight through simulation of requisite complexity

The argument here combines points made in earlier discussions (*Ambiguity of "democratic oversight": institutionalisation of negligence?* 2013; *Simulation of consequences and possibilities of cognitive engagement*, 2013).

Restricted focus of current simulations: Dating from the pioneering efforts of the Club of Rome publication of *The Limits to Growth* (1972), there have been a variety of approaches to the simulation of the nature of the "problematique" and the possibilities of a "resolutique" (*Club of Rome Reports and Bifurcations: a 40-year overview*, 2012). Missing has been any adequate exploration of the nature of the failure of remedial action, as argued separately (*Recognizing the Psychosocial Boundaries of Remedial Action: constraints on ensuring a safe operating space for humanity*, 2012). This pattern is reflected in the most recent report to the Club of Rome (Johan Rockstrom and Anders Wijkman, *Bankrupting Nature: Denying our Planetary Boundaries*, 2012).

In particular there has been a failure to incorporate "embarrassing" issues into simulations, especially those relating to population dynamics (*Map of Systemic Interdependencies None Dares Name: 12-fold challenge of global life and death*, 2011; *Mapping the Global Underground: articulating Insightful Population Constraint Consideration (IPCC)*, 2010). Also missing is their relationship to the process of electing creativity and to the destabilizing effects of (bureaucratic) game-playing. To complement the "problematique" and the "resolutique", these might be framed as an "imaginatique" and a "ludique" -- in considering the possibility of understanding in terms of complex system dynamics (*Imagining the Real Challenge and Realizing the Imaginal Pathway of Sustainable Transformation*, 2007).

These challenges are relevant given the considerable resources now being allocated to new forms of simulation -- questionably related to the data mining commitments of the security services (as mentioned above). Notable initiatives include:

- the GDELT Penn State Event Data Project (*Global Data on Events, Location and Tone*)
- the projected "Living Earth Simulator", of the FuturICT EU research initiative "to explore social life on earth and everything it relates to".

The question may well be asked whether current simulations are effectively designed as exercises in conceptual gerrymandering -- to avoid consideration of issues fundamental to any remedial capacity. In this sense they can be accused of being as much part of the problem as of the solution -- especially in relation to the adequacy of democratic oversight.

Appropriate questions? The challenge can be represented otherwise when consideration is given to the nature of the questions which might be asked of the supercomputers required for such simulations, especially those of the NSA, as discussed separately (*Superquestions for Supercomputers: avoiding terra flos from misguided dependence on teraflops?* 2010).

The nature of the disclosures regarding the secret NSA/PRISM data mining and intelligence sharing agreements, and the extent to which internet service providers are effectively "front-ends" for such processes's, suggests that emerging supercomputer projects (such as those above) may also function as "front-ends" -- whether knowingly or unknowingly.

Given the above-mentioned reliance on legislative "oversight" to guard against abuse, **what provision is made for simulating oversight in terms of its effectiveness with case loads of varying sizes and complexity, involving oversight committees of different sizes, or the possibilities of loopholes** (as noted above)? Could vulnerabilities to oversight failure be detected -- as possibly exacerbated by human error, incompetence, and conflict of interest? **How might such simulation contribute to appropriate risk analysis with respect to a vital systemic role?**

The current controversy over the "least truthful answer" made in response to questioning by James Clapper, US Director of National Intelligence, offers an example (*James Clapper: Obama stands by intelligence chief as criticism mounts*, *The Guardian*, 12 June 2013). As presented by David Sirota:

James Clapper is now the embodiment of perjury before Congress. Indeed, when you couple Edward Snowden's disclosures with the video of Clapper's Senate testimony denying that the National Security Administration collects "any type of data on millions (of Americans)," Clapper has become American history's most explicit and verifiable example of an executive branch deliberately lying to the legislative branch that is supposed to be overseeing it. (*James Clapper Should Be Fired -- And Prosecuted*, *AlterNet*, 12 June 2013)

Simulating oversight functions: The controversy has evoked discussion over how exactly the oversight is ensured (*Paddy Ashdown, NSA surveillance: who watches the watchers?* *The Guardian*, 12 June 2013). The quality of the points made, and the associated comments in that example, are an indication of how simplistic is the apprehension of the matter in comparison with its possible complexity. Hence the case for simulation to enable and inform more adequate discussion regarding oversight provisions.

As noted above, the effectiveness of the oversight function might be formulated otherwise through questions such as: **would members of oversight committees be prepared to travel in a plane subject to the quality of safety checks characteristic of their own oversight procedures?** Exploiting that vehicle safety metaphor, for the wider population the question can be related to that of the trustworthiness of used car salesman, as highlighted by a recent survey which noted that the only profession that Americans trusted less than Congressmen was used car salespersons (*Car Salesmen Trusted Even Less Than Congressmen: Gallup*, *The Huffington Post*, 3 December 2012). Presumably it is "Congressmen" who are represented on oversight committees in the USA. The issues can be related to the concerns regarding "intelligence failure" prior to 9/11 -- as documented by a *US Senate inquiry* (cf Kjetil Anders Hatlebrekke and M. L.

R. Smith, *Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure, Intelligence and National Security*, 2010).

Detecting vicious cycles and loopholes: The issue is whether such data mining and simulation can address the possibility of "vicious cycles". and assist in "breaking" them (*Dysfunctional Cycles and Spirals: web resources on "breaking the cycle"*, 2002). In metaphoric terms the challenge might be framed in terms of the capacity to detect whether civilization is effectively "walking in circles" in a strategic desert -- and whether appropriate creative thinking and relationships can be enabled as separately suggested (*From ECHELON to NOLEHCE: enabling a strategic conversion to a faith-based global brain*, 2007).

In their use by the "intelligence agencies", simulations are notably valued for their potential capacity to detect terrorist groups and rings. Of great interest is whether such simulations are capable of detecting dysfunctional behavioural loops embedded in networks of perceived problems and collective initiatives. Pointers in that direction have been offered by a EU-funded development of the databases of the *Encyclopedia of World Problems and Human Potential* as separately described (*Feedback Loops Interlinking World Problems and Global Strategies*).

This notably experimented with the software produced by *Netmap Analytics*, specifically designed to detect questionable patterns of interaction in the kinds of transactional meta-data currently collected by the NSA (*Preliminary NetMap Studies of Databases on Questions, World Problems, Global Strategies, and Values*, 2006; *Visualization: Holistic network mapping using NETMAP*, 1995). The early experiments with analysis of such complex networks gave rise to a proposal by a university in the USA, involving the developers of Netmap, for a Global Knowledge Grid ("a new infrastructure for understanding globalization") -- effectively a precursor of the Penn State Event Data Project (mentioned above).

Improvement of "oversight" capacity merits detailed verification of that process through simulation -- given the human cognitive constraints in relation to such vast quantities of data and the highly problematic dynamics of any oversight committee process. Appropriate simulation would ensure appropriate **feedback loops** to confirm the integrity of the process -- in the light of cybernetic insights (as noted above). As with "oversight" itself, there is however a delightful irony to the fact that "leaks" occur through "**loopholes**". In mathematical terms, these may be of higher dimensionality than is normally assumed or readily understood. The concern is occasionally compared metaphorically to the holes in a Swiss cheese, as with the argument of Euro-MP Dennis de Jong (*EU Banking Regulation 'as full of holes as a Swiss Cheese'*, *SP International*, 16 April 2013) or that of Eliot Spitzer (*Romney's tax plan is Swiss cheese: full of holes*, *The Cap Times*, 21 October 2012).

Crowdsourcing: Such simulation could be fruitfully related to the more general issue of the manner in which solicited "democratic feedback", and proposals for "alternatives", are systematically ignored (*Considering All the Strategic Options -- whilst ignoring alternatives and disclaiming cognitive protectionism*, 2009; *Enabling Collective Intelligence in Response to Emergencies*, 2010). There is of course no lack within the NSA environment of the relevant skills to design such a simulation -- although a higher order of oversight would also be required to ensure that **backdoors** were not inserted to enable the process to be "tweaked" (as with some electronic voting processes).

The whole question of "democratic oversight" of intelligence services calls for simulation capable of highlighting the vulnerabilities best described by "setting the fox to guard the chicken coop", a phrase widely used in several variants in relation to government (Molly Ivins, *Fox Guards Henhouse in Bush's Selections*, *The Dispatch*, 25 August 2001).

The argument is remarkably developed in a well-illustrated presentation by Kimmo Soramäki (*Simulation Analysis and Tools for the Oversight of Payment Systems*, *Latin American Center of Monetary Studies*, 2012) as a means of clarifying the system of financial transactions implicated in the financial crisis. It is introduced by remarks of *Jean-Claude Trichet*, President of the European Central Bank;

When the crisis came, the serious limitations of existing economic and financial models immediately became apparent.... As a policy-maker during the crisis, I found the available models of limited help. In fact, I would go further: in the face of the crisis, we felt abandoned by conventional tools. (18 November 2010)

The case of Edward Snowden is a useful challenge for exploring the ambiguities of "democratic oversight". On the one hand his actions revealed the insecurity "holes" in what might have been assumed to be a Six Sigma system. On the other hand, his initiative was purportedly in the interest of ensuring "democratic oversight" -- by the peoples of the US. Is Snowden effectively an embodiment of "democratic oversight" in both senses of the term? The founder of the e-mail service, reportedly used by Snowden, closed it down with the suitably ambiguous declaration that he would not be complicit in "crimes against the American people" (Spencer Ackerman, *Lavabit email service abruptly shut down citing government interference*, *The Guardian*, 9 August 2013). To what extent should a simulation encompass both the possibility of leaks and efforts to enable democratic transparency, however misguided?

Unknown unknowns: Ironically the challenge of "democratic oversight" of electronic surveillance is highlighted by the "**poem**" notoriously presented by *Donald Rumsfeld* as US Secretary of Defense in February 2002, and discussed separately (*Unknown Undoing: challenge of incomprehensibility of systemic neglect*, 2008):

*There are known knowns;
there are things we know that we know.
There are known unknowns; that is to say,
there are things that we now know we don't know.
But there are also unknown unknowns -
there are things we do not know we don't know.*

Transforming from paranoia through metanoia and hyponoia?

Concluding section presented separately as an annex: [Transforming from paranoia through metanoia and hyponoia?](#) with separate references.

References

Kurt Eichenwald. 500 Days: Secrets and Lies in the Terror Wars. Touchstone, 2012

Michael E. Mann. The Hockey Stick and the Climate Wars: dispatches from the front lines. Columbia University Press, 2012

Thomas E. Mann and Norman J. Ornstein. It's Even Worse Than It Looks: how the American Constitutional System collided with the new politics of extremism. Basic Books, 2012

Naomi Oreskes and Erik M. Conway. Merchants of Doubt: how a handful of scientists obscured the truth on Issues from tobacco smoke to global warming. Bloomsbury Press, 2011

Robert B. Reich. Beyond Outrage: what has gone wrong with our economy and our democracy, and how to fix it. Vintage, 2012

Philippe Sands:

- Lawless World: America and the Making and Breaking of Global Rules. Viking Adult, 2005
- Torture Team: Rumsfeld's Memo and the Betrayal of American Values. Palgrave Macmillan, 2008

Larry Siems. The Torture Report: what the documents say about America's post-9/11 torture program. OR Books, 2012 [[text](#)]

Nassim Nicholas Taleb:

- The Black Swan: the impact of the highly improbable. Random House, 2007
- Antifragile: things that gain from disorder. Random House, 2012

Pablo Triana and Nassim Nicholas Taleb. Lecturing Birds on Flying: can mathematical theories destroy the financial markets? Wiley, 2009



This work is licensed under a [Creative Commons Attribution-NonCommercial 4.0 International License](#).

For further updates on this site, [subscribe here](#)