An Evaluation of the Total Information Awareness (TIA) Project

Alex Burns (alex@disinfo.com), June 2006

Abstract

In 2002 the Defence Advance Research Projects Agency (DARPA) conceived an embryonic counter-terrorism system to deal with post-September 11 intelligence reforms. Total Information Awareness (TIA) integrated technology solutions from databases, expert systems and natural language processes to enable predictive capabilities in a multi-agency environment. TIA faced intense scrutiny from civil liberties and privacy advocates once the research program's details were made public. These ranged from Cato Institute and Heritage Foundation policy critiques to blogosphere attacks on Vice Admiral John Poindexter, the director of DARPA's Information Awareness Office (IAO). DARPA repositioned TIA as Terrorism Information Awareness before ending it and closing IAO in late 2003. This essay provides a post-mortem that evaluates the TIA project and its social controversies, and derives design lessons for future intelligence systems.

Key Research Questions

· Why did DARPA propose TIA in the post-September 11 security environment?
· What factors led to TIA's failure? What lessons may be learnt for future projects in the Intelligence Community on the design of distributed information systems and analytical support tools?
· What role did civil society alliances, media narratives, and policy networks play in the TIA 'scandal'?

Introduction

This research paper conducts a project post-mortem on the Total Information Awareness (TIA) system, a prototype Information System for counter-terrorist intelligence. TIA was conceived in financial year 2002 by the Information Awareness Office (IAO), a former Research & Development (R&D) office of the United States-based Defense Advanced Research Projects Agency (DARPA).[1] TIA's systems architecture was conceived as part of a 'full spectrum' solution for decision-making support which included capabilities in data-mining, language and expert systems. TIA's developers believed it would provide analytical support within the multi-agency US intelligence system.

As a case study TIA provides one avenue to evaluate the intelligence reforms undertaken since Al Qaeda's terrorist attacks against the US on 11 September 2001. TIA's diffusion failure also provides lessons on a range of broader issues that include the role of design, the complexity of socio-technical systems, R&D for national security and privacy rights. The media controversy over TIA's goals and means involved a wide range of strategic actors who influence the ecosystem that the Intelligence Community (IC) operates within. The emergence of new actors has implications particularly for how intelligence agencies handle risk communication. Finally, TIA's design involved several emerging technologies which may affect the way collections, processing and analytical stages of the Intelligence Cycle are undertaken in the future.

Research Issues

The author confronted several key research issues in this essay.

First, TIA information is scarce due to the intelligence nature of the project and the fact that it only proceeded from the analysis to design phase. Several other systems that may be operational are mentioned below.

Second, the controversy has meant that DARPA redacted TIA information from its official site and closed the Information Awareness Office (IAO) that oversaw the project. Some of this information was recovered using the Wayback Machine (www.wayback.org) although it is not complete. This information was for public distribution only and does not likely reflect the views of DARPA's internal staff.

Third, the TIA information has been reframed by various strategic actors in the IC ecosystem. Whilst this offers richly multi-perspectival viewpoints about TIA's potential effects, it also obscures how the IC perceived it, and how the technology architecture would have been integrated into intelligence planning and processing. Finally, the essay is limited by the author's understanding of IC issues and requirements analysis techniques. Critical reflections are offered below in the section on Conclusions and Further Research, and in Appendix 1.

The Post-September 11 Environment and TIA's Design

The post-September 11 environment imposed several drivers and influences on TIA's design. The September 11 attacks raised policymakers' awareness of critical uncertainties and emerging threats in a global security environment.[2] The National Commission on Terrorist Attacks Upon the United States (hereafter the 9/11 Commission) echoed the Aspin-Brown Commission and earlier studies in seeking reforms to the IC's national structure and institutions.[3]

The 9/11 Commission's recommendation to build a "trusted information network" was especially relevant for TIA's developers.[4] However, the 9/11 Commission's report scope did not cover the possible misuse of analytic product by US policymakers. Although the works of Janis, Kahneman and Tversky on decision-maker biases were well known, more pernicious explanations such as market deregulation failure of the airline industry and the influence of special interest groups have been largely overlooked.[5] Despite these unexplored issues the US IC prioritised the need for an integrated system to handle collection management and intelligence dissemination.

An in-depth analysis of the intelligence reforms literature is beyond the scope of this essay. However, several key contributions to the literature should be noted for their implications. Steve Coll's genealogy traces the emergence of Al Qaeda from the Soviet invasion of Afghanistan in 1979 to 10 September 2001.[6] Sandra Silberstein's content analysis of the three-week transition from September 11 to the US reprisal bombing of Afghanistan suggests a vengeance-motivated escalation, beyond the dominant theory of neoconservative influence.[7] Policymaking histories by Daniel Benjamin and Richard Clarke mix Administration insights and IC reform proposals with dystopian threat scenarios.[8] Robert Baer's work offers an IC counter-critique from a field agent's perspective.[9]

From different perspectives, this literature contends that September 11's causes were a complex mixture of agendas, blind-spots and long-term problems within the IC. For many analysts, the late Federal Bureau of Investigation agent John O'Neill personified these issues, having unsuccessfully fought with FBI Director Louis Freeh's managerial cohort to track Al Qaeda from Khobar Towers (1996) to the USS Cole bombing (2000).[10] Technological solutions would be unable to accommodate dissidents such as O'Neill in high-velocity crisis circumstances. Ironically, the 9/11 Commission's immersion in Bush Administration politics also spurred the 9/11 Truth Movement's creation. This alliance—of September 11 victims' families, socio-political activists and IC dissidents—have sought different explanations, and were part of the civil society network that decried TIA's operational deployment.

DARPA and TIA's Technological Imperative

In the early 1990s IC reformists looked to the business community for lessons on finding a new purpose. For William Odom, the IC's bureaucratic model had prevented process reengineering and other transformative initiatives from occurring, particularly in technical solutions to the collections phase.[11] TIA updated this thesis for the post-September 11 environment, where R&D contracts were closely linked with boutique security firms such as Booz Allen Hamilton.[12]

Publicly available briefings on TIA outline a technology mix conceived to anticipate and pre-empt future terrorist threats.[13] Vice Admiral John Poindexter, the IAO program manager responsible for the TIA project, noted that database and data-mining technologies were chosen to globally scan the "transaction space" that might reveal potential terrorist attacks underway.[14] Poindexter's comment reflects the widespread knowledge of the Phoenix Memo's failure to mobilise the pre-September 11 IC, and the visibility of Enterprise Resource Planning vendors for large-scale Information Systems solutions.[15] His presentation slides for DARPATech 2002 emphasise TIA's capabilities in thwarting "asymmetric threats", the primary IC sound-bite in the months after September 11.[16]

Requirements Analysis of TIA is bounded by such publicly available information. Poindexter's slides reveal a systems architecture based on the augmentation of traditional intelligence with "collaborative analysis" and "collaborative response" cycles. This analytic environment is supported by "automated data stores" which process security "authentication" and filtered "transactions". TIA's system architecture encompassed a number of sub-projects on knowledge extraction, real-time translation, war-gaming decision models and speech-to-text filters.[17] The database approach had been influential in early 1980s projects designed to provide the IC with Overt Source Intelligence on power projection cross-comparisons and country studies.[18] However, it is unclear if DARPA's designers worked closely to develop robust links between the analytical environment and TIA's transaction processing engine, beyond this early model. Existing studies by IT experts of TIA's requirements have limited value, because they model domains and systems architectures that fail to encompass IC's contexts and needs.[19]

DARPA's emphasis on TIA's technological dimensions ran counter to the Information Technology's wisdom community. First, DARPA positioned TIA to the general public as a "silver bullet", coined by IBM /360 project leader Fred Brooks to describe technology solutions that over-promised solutions to complex socio-technical systems.[20] In his essays 'No Silver Bullet' (1975) and 'No Silver Bullet - Refired' (1988), Brooks rejects the vendors' frequent claim that technology-driven solutions would create ten-fold productivity increases. Second, Brooks' insights are reflected by cryptographer and security expert Bruce Schneier, who warns that technology-driven solutions are the weakest link within intelligence systems, and susceptible to errors.[21] TIA's project failure also reflected a norm within the Information Technology industry. According to the Standish Group's annual *CHAOS Report*, which since the early 1980s has tracked the metrics and reasons for IT project failures, the implementation failure rate has hovered around 60 percent.[22]

Perspectives from Science, Technology and Society literature raise several concerns about TIA's systems architecture as Poindexter described it. Andrew Feenberg captures the limits of technical rationality when he invokes "Design Critique" as a perspective which "holds that social interests or cultural values influence the realization of technical principles."[23] Alexander Galloway extends Feenberg's thesis, drawing on Gilles Deleuze and Felix Guattari's neo-Marxist analysis to raise concerns about the control of decentralised network structures.[24] Civil society advocates with 'oppositional' politics to the IC had similar views. Finally, Charles Perrow's research into disasters and tightly-coupled systems is relevant to how TIA would have been integrated into IC agency workflow.[25] Despite this, Bruce Berkowitz and Allan Goodman believe the IC has not learnt from Perrow's work and other disasters.[26]

A 16 November 2002 editorial in *The Washington Post* emphasised the views of these authors when it noted that despite DARPA's claims, "this is not neutral technology, and the potential for abuse is enormous."[27] Shannon R. Anderson, a researcher with the Bill of Rights Defense Committee, noted that key dangers in using data-mining included the impact on Constitutional rights, transparency limits and concerns about "false positives."[28] These views are a sample of the concerns raised about TIA throughout late 2002 and early 2003 (summarised in Appendix 2).

Issues With TIA's "Collaborative Analysis & Response" Cycle

The second unresolved major problem with TIA's systems architecture involves the epistemology of its "Collaborative Analysis" and "Collaborative Response" intelligence cycle. Poindexter and others sought to portray TIA's databases, query-driven expert systems and security measures as comparable to Dee Hock's 'chaordic' design for VISA transactions. Yet TIA's chokepoints are the "Filters" in its transaction processing system, and the "Decisions" engine in its analytical support area.

Computer Science paradigms in artificial intelligence and mathematics have a rich tradition in expert systems and machine learning tools which can search data for significant patterns. The codification of problem domain knowledge and epistemic frameworks becomes vital in such endeavours. There are now a bewildering array of Monte Carlo and other risk simulators. Programmers have also turned to Object-Oriented (O-O) programming as a way to translate this knowledge and frameworks into computer code. O-O analysts have consequently adopted models from anthropologist Gregory Bateson, architect Christopher Alexander and others to create more dynamic "pattern languages" that can capture the dynamical change and fluidity of real-world phenomena.

O-O code is designed to reflect the stability of behaviour classification, domain classes and relational taxonomies. While such criteria can certainly identify the structure and attributes of IC processes, it is much harder to apply these distinctions to modelling terrorists and organisations which are adaptive, fluid and even context-dependent. Consequently, counter-terrorist researchers such as Jessica Stern and Michael Scheuer are turning to self-reflexive techniques and hermeneutic lifeworlds to explain terrorist motivations.[29]

Unable to handle this dimension O-O programmers look instead for externally observable state-changes such as "transaction space" signals. Yet this approach then minimises the counter-intelligence and operational security dimensions of both terrorists and the IC agencies that pursue them. It is also difficult to perceive how such a system could evaluate the "received wisdom" about a situation without close involvement by the intelligence team.[30] Instead, the IC databases that TIA was attempting to replace have a wealth of tactical data and Signals Intelligence that requires frequent updating.[31]

One alternative would have been for TIA's designers to model the analytic environment as a participatory "information ecology."[32] This reflects the Intelligence Augmentation tradition (IA) pioneered by J.C.R. Licklider's cyborg research in the 1960s, and Douglas Engelbart's influential work on coevolutionary design.[33] An IA paradigm would shift the developer's attention back to the IC analyst, and how the systems architecture would affect their attention span and cognitive style.[34] For example, IA could extend the emerging frameworks on how individuals and groups process information in ambiguous environments.[35]

The IC Ecosystem and Norm Contestation in the TIA Debate

The TIA debate illustrates the complexity of the Intelligence Community ecosystem within the United States and the role of different strategic actors. Debates and norm contestations are shaped by several factors—the institutional structure of the US intelligence system, awareness of the 1975—1976 Church Committee hearings, and the libertarian tradition in socio-political activism—means that TIA had greater public scrutiny than the Royal Commission model used in Australia and the United Kingdom. These debates mirrored the 'frame wars' that linguist George Lakoff has used to analyse US political debates.

The TIA debate included the following strategic actors:

- *The Agenda-Setting Media*: Agenda-setting publications such as *The New York Times*, *The Washington Post* and CNN have specific journalists to cover counter-terrorism, national security and technology-related issues.[36] This meant these publications engaged in a more spirited debate about TIA than in countries where media outlets are more centralised and journalists are not as closely involved in these issues. National opinion magazines were also involved from a variety of viewpoints: the left (*Harpers*, *The Nation*), centrist (*The New Republic*), libertarian (*Reason*), and the right (*National Interest*, *The Weekly Standard*). Viewpoints on TIA varied, with *The National Review*'s Jonathan Levin expressing a minority view that TIA was necessary given DARPA's past research successes, and its leveraging of FBI-style behavioural profiling to identify potential terrorists.[37]

- *Policy Think-tanks*: The TIA case attracted the attention of policymakers and strategists in several high-profile US sites. The polarised responses reflected the perceived dominance of conservative and right-wing think-tanks in the US on IC and national security issues. The Cato Institute's Gene Healy looked to American fears of German saboteurs in World War I as one historical analogy.[38] The Heritage Foundation's Michael Scardaville countered the popular media analogy which equated TIA with George Orwell's novel *1984*.[39] These different positions provided a snapshot of similar debates in the agenda-setting media.

- *Privacy Groups*: Internet and privacy lobby groups have been involved in several IC cases, and in wider debates such as the Clinton Administration's 'Clipper' chip and the Digital Millennium Copyright Act. The Electronic Freedom Foundation (EFF) and the Electronic Privacy Information Center (EPIC) have extensive mini-sites on the TIA incident with commentary and news. Cryptome also offers TIA resources and analysis of IT and privacy-related issues.

Many of these groups were motivated by oppositional politics to the IC, and TIA's design reliance on the data-mining of databases, a weakness identified in other high-profile cases of consumer credit card leaks. These sites are discussed below concerning some ironic digital continuity outcomes. The American Civil Liberties

Union and similar lobby groups viewed the impacts on human rights with alarm.[40] Legal scholars such as Anita Ramasastry contended that TIA's system would in effect create "digital profiling."[41]

• *Digerati Libertarians*: Many of the influential Internet theorists, who had co-formed the privacy groups discussed above, also waged a campaign against TIA's deployment. John Perry Barlow believed that DARPA's technology history meant that TIA could actually happen.[42] Stowe Boyd looked to Social Network Software sites such as Friendster and LinkedIn to provide TIA-like capabilities for advertising agencies.[43] Howard Rheingold praised the US Senate's decision in late January and early February 2003 to end DARPA's funding for TIA.[44]

• *Independent Researchers*: Libertarian advocates such as The Memory Hole's Russ Kick and the US conspiracy community provide archives and commentary on TIA and other incidents. The first can be viewed as a 'wild card' for the IC similar to 'lone wolves' in counter-terrorism discourse. The second group was incensed by DARPA's decision to include a logo and vision statement ("Scienta Est Potentia"(?)) which was interpreted as Illuminist politics.[45] This group raised the personality politics around director John Poindexter that created embarrassment for DARPA, an 'attack PR' model of dealing with emerging crises.

• *'Outsider' IC Members*: This category has several sub-groups. TIA attracted commentary from former IC field agents and analysts such as Robert Baer and Ray McGovern in the US. The former NSA analyst Andy Dunn compiled a genealogy for the leftist *Z Magazine* which linked TIA's agenda to the FBI's disgraced COINTELPRO and earlier perceived excesses of collections and counter-intelligence.[46]

Although each group had different concerns about DARPA's intentions, they had commonality in recognising that TIA's system architecture was not congruent with the post-September 11 realities. The implications and outcomes for privacy of information and process design were unclear. The procedures for transaction processing, database access and privacy controls were not well-formed solutions.[47] TIA remained unclear to IC outsiders who did not share DARPA's zeal for its counter-terrorism intelligence solution. Ironically, the archives of independent researchers and privacy groups are now the main public source for TIA project information.[48]

Flashpoint: The John Poindexter Incident

The controversy over Vice Admiral John Poindexter's role in DARPA as TIA's program manager exemplifies how norm contestation between strategic actors can influence the IC ecosystem. Poindexter was viewed as representative of the Bush Administration's intrusion of executive powers into the IC. *The Christian Science Monitor* and other agenda-setting media recalled his involvement in the Reagan Administration's Iran/Contra scandal in 1986.[49] Meanwhile, Digerati libertarians such as *TechTV* and *Wired* covered the Internet campaigns against Poindexter's appointment.[50] Technology journalist Annalee Newitz dubbed Poindexter's initiative the 'Totalitarian Information System', highlighting how the project's support was split along Democrat—Republican lines.[51]

The situation escalated when *SF Weekly* columnist and 'culture jammer' Matt Smith managed to uncover Poindexter's address and phone number, then publicly disclosed them.[52] The incident also highlighted how past IC controversies can be reignited in current debates. Shortly afterwards, DARPA took steps to reframe TIA as 'Terrorism Information Awareness', and to avoid further public embarrassment. Poindexter subsequently closed DARPA's IAO office. Such circumstances prompted *The New Yorker*'s Hendrik Hertzberg to compare Poindexter's situation with a surreal Philip K. Dick novel.[53] The Center for Public Integrity's Charles Lewis continued this media narrative with a comparison to Rod Serling's *Twilight Zone* program.[54]

The focus on Poindexter has obscured how different strategic actors were able to reframe the TIA debate, and to change the IC ecosystem through pressure on Congressional legislative oversight. On 31 December 2003 the Department of Defense's Office of the Inspector General released a Report, dated 12 December 2003, on TIA's oversight. The Report's recommendations included the appointment of a "Privacy Ombudsman" and for DARPA to conduct "a privacy impact assessment" on future projects.[55] IAO was closed down soon afterwards and DARPA dropped TIA from its public coverage.

Aftermath: Google As TIA II?

TIA represented an IC model to deal with the collections and processing demands of the post-September 11 era. Ironically, the controversy was sparked in part by its design: a closed system with access to public databases. For some analysts, TIA's design has already been rendered near-obsolete by the popular Internet search-engine Google (www.google.com).

Google's algorithm and dominance of the search-engine market has turned it into a powerful tool for Overt Source Intelligence (OSI) gathering. When combined with archive tools such as the aforementioned Wayback Machine, Google provides the ability to cache information, search for keywords, and to monitor global media and news feeds on a near real-time basis. This power has made Google legendary: David Vise's organisational history and John Battelle's 'Database of Intentions' reflect several of TIA's design elements in a more utopian worldview.[56] These capabilities have created an online environment closer to David Brin's vision of a 'transparent society' which alters our conception of privacy rights.[57]

However this success and Google's increasing control of the search-engine market has created a backlash. Google's founders Sergey Brin and Larry Page have been likened to Microsoft's Bill Gates. This backlash parallels Geoffrey Moore's marketing observation that companies can lose audiences when they 'cross the chasm' from the visionaries/early adopters to the mainstream.[58] Google's decision to list on the New York Stock Exchange also attracted critics who believed that its innovation culture was unsuited to the rigorous demands of the business environment.

Brin and Page have attracted criticism over a range of issues, from Google's compromise with the Chinese Government over censorship, to the potential for the Google Maps service to be used for Signals Intelligence collection. Just as with the Poindexter incident, Brin and Page are now targeted by human rights and privacy activists. Google deserves its own intelligence case study: relevant issues include the US—China geostrategic tension, the different priorities of national intelligence systems, and the 'wild card' impact of controversial groups such as Falun Gong.

In the near-term future, the period after September 11 may be compared with the 1975—76 Church Committee's reforms to US policies on assassinations and covert action. TIA-style scandals have now enveloped the National Security Agency and will surely trigger new investigations. *New York Times* journalist James Risen has revealed the NSA's Signals and Technical Intelligence programs have been used to bypass Constitutional limits on wire-tapping. Digerati libertarians have again played an oppositional role to the IC, with *Wired* News publishing the affidavit of AT&T whistleblower Mark Klein, about a backdoor program to redirect Internet traffic to the NSA for processing.[59] The TIA and NSA incidents promise future IC scandals for years to come. As one final twist, during the confirmation hearings for the CIA's new Director-elect, General Michael Hayden, he stated that he would answer questions about TIA and the NSA only in a "closed session" likely to be held in a Specially Compartmentalised Intelligence Facility.[60]

Conclusions and Further Research

The TIA case was instrumental in raising public awareness about post-September 11 initiatives by the IC to deal with terrorist threats. This section is divided into three main areas: General Trends, Lessons Learnt for the Design of Future Systems, and Future Research. Further insights and reflections are included in Appendix 1.

The conclusions are divided into three main areas: general trends, the IC and risk communications strategies, and lessons learnt for the design of future systems.

1. General Trends

Post-September 11, IC agencies have placed greater emphasis on Overt Source Intelligence and links with the business community. For OSI pioneers such as Robert David Steele, this signifies growing legitimation by the IC community that has taken over a decade to occur. The Australian Security Intelligence Organisation and the Central Intelligence Agency have each now established dedicated organisational groups for OSI-related work. This may signal a shift by the IC community to incorporating the most relevant aspects of the OSI and Open Source communities into their practices.

However, the warp-speed nature of Internet information flows means that IC agencies will continue to face internal pressures to maintain the "need to know" principle. These pressures will challenge OSI's "distributed intelligence" paradigm. Consequently, one outcome of TIA and similar incidents may be a renewed focus on risk communication plans that underpin counter-intelligence and security vetting procedures. This particularly extends to the unauthorised disclosure of document metadata and publication authorisation processes. In turn, civil society advocates and hacktivists will seek to develop new tools to un-redact this information.

2. Lessons Learnt For The Design Of Future Systems

Although TIA was a failure, it provided many lessons that can be integrated into the requirements analysis and design phases of future systems. Attention to the development and system deployment environments will be critical to avoiding diffusion problems within IC institutions.[61]

Future IC systems should provide an evaluation at the planning stage of the technological architectures and solutions that the project will deploy. This evaluation should explore the technology mix and its implications from end-user and IC needs, rather than rely on vendor demonstrations. It should draw on IC experiences and reflections rather than impose top-down solutions, and should engage a wider range of strategic actors.

The effective project management of IC systems must strengthen the Quality Assurance (QA) processes. In a post-Enron environment QA checks and balances must include clarity of processes and workflows, internal checks and external auditing. This could reinvigorate IC oversight mechanisms in a similar fashion to how the Enron and Worldcom scandals led to corporate governance initiatives like the Sarbanes-Oxley compliance legislation. For IC systems that are designed to monitor public information, this requires access and usage monitoring, 'dirty data' cleaning and encryption, and attention to potential abuses.

3. Further Research

Disclosure of more information about TIA could lead to a revision of the Requirements Analysis models used in this essay, which was limited by publicly available information. R&D scientists and senior staff have not yet commented on the TIA program. This could add new details and critical reflections to the case, particularly if cross-compared with IC views on problem domain modelling. The IC's protocols on operational security and tradecraft mean that a full picture of TIA's capabilities and processes is unlikely to be truly known.

Despite these barriers, specific methods could be developed for socially-driven Requirements Analysis and Reverse Engineering that meets IC needs in the counter-terrorist problem domain. David West's "domain anthropologist" approach is one solution, where systems designers work closely with Subject Matter Experts in fieldwork to capture tacit and unconscious insights.[62]

The 'frame wars' dimension of the TIA debate suggests that future case studies need to have a multi-perspectival viewpoint to understand the strategic actors and their intentions. This may identify communication patterns and structures that can be used to more effectively convey the intentions and operational realities behind the systems. By considering all perspectives and positions, a more integrative solution can be developed. Whilst such exercises need to be bounded, a failure to explore this can lead to blind-spots, groupthink and other well-documented problems within the IC cycle.[63]

Appendix 1: Post-Mortem Lessons

The Total Information Awareness project failed due to several reasons:

1. DARPA failed to deal with the flak from civil society advocates and critics. Once *Wired* News, *Slashdot* and ‘blogosphere’ sites such as *The Daily Kos* discovered TIA and Vice Admiral John Poindexter’s role, they fashioned a media counter-narrative that pressured the US Congress and DARPA project stakeholders. This media counter-narrative mobilised a range of strategic actors who reframed the broader debate and pressured the US Government in its legislative oversight role to shutdown the TIA project.

2. TIA’s systems architecture reflected a range of influences from the historical influence of cybernetic models and functionalist philosophy in Computer Science to contemporary concerns about anti-money laundering and state-sponsored terrorism. Despite this ambitious agenda, TIA’s systems architecture and sub-projects were not communicated clearly in a way that dealt with concerns about data control and privacy. Second- and third-order effects of sub-project technologies were not publicly debated in an adequate fashion. Data control, privacy and security issues need to be integrated into Requirements Analysis and Design phases, rather than left until the later Implementation deployment phase to be resolved.

3. TIA’s approach to terrorist identification was based on database, data mining and profiling technologies. This combination would create fear amongst civil society advocates which had viewed them as ‘hot button’ issues due to customer relationship management applications in a business context. EPIC and other netizens took up TIA as a *cause celebre* to deter and deny. The audit trail and corporate governance functions were not detailed enough in a multi-agency environment that required clarification. These systems were also designed to look for terrorists as a series of cascading events and threat thresholds rather than an unfolding process.

4. TIA’s construction of terrorist identity was too simplistic. The post-September 11 reaction to intelligence failures such as revelations about the FBI Phoenix memo led

to an emphasis on pattern matching from public sources. This systems design was predicated on the assumption that future terrorist cells would follow similar actions, and that the signals could be collected, sorted and prioritised separate from public information. TIA's public designs appear to draw on Artificial Intelligence expert systems without attention to how the Counter-Terrorism problem domain is codified in Object-Oriented modelling. It ignored the self-reflexive models of key researchers—amongst them Mark Juergensmeyer, Marc Sageman, Andrew Silke and Jessica Stern—which considered the constructivist and inter-relational dimensions of terrorist motivations, groups and movements.

5. TIA and the related Terrorism Futures Market project both recognised the need for anticipatory risk communication. However, the methodologies chosen—scenario planning, asymmetric war-gaming, and capital market simulations—have assumptions and biases that often failed to capture the realities noted above. Their sensationalistic media portrayal also eroded any public support for their open application. Other methodological options were not explored, nor were Subject Matter Experts consulted in the Futures Studies and Strategic Foresight communities of practice.

Design and Systems Development Life Cycle (SDLC) Lessons

1. Domain knowledge is critical in the analysis and design phases of a systems architecture. A system designed with awareness of critical security studies and counter-terrorism would have led to very different solutions. The 'flawed epistemology' of earlier counter-terrorism models meant an emphasis on publicly sourced profiling, a decision also possibly made as retroactive management due to September 11 investigations. Although multi-agency capabilities were outlined in TIA schematics, it remains unclear if these multi-sectoral end-users were engaged in the requirements gathering process.

2. TIA was conceived in a research context shaped by Government considerations about Science & Technology exercises. Its design reflected a transitional Cold War era mentality about intelligence culture rather than the cutting edge. This may have also reflected a Department of Defense-mandated 'waterfall' project model, rather

than Agile iterative approaches that involve multi-agency end-users in the Requirements Analysis phase.

3. Its IC focus meant that TIA was conceived as a closed rather than an open system. Whilst this may have been appropriate in the IC context, this design set TIA at odds with the Open Source software community and Digerati libertarians. Database and transaction processing in TIA’s systems architecture created a perception that it was the Orwellian archetype of secret pattern matching from public data. Alternatives such as Overt Source Intelligence and Citizen Journalism were not explored at this early stage and integrated into the design.

Appendix 2: Partial Timeline of TIA Events

Circa January 2002	DARPA's Information Awareness Office (IAO) begins the Requirements Analysis phase for the Total Information Awareness project
2 August 2002	John Poindexter reveals TIA during DARPATech2002.
13 August 2002	DARPA begins to award commercial contracts for TIA research, including Booz Allen Hamilton
9 November 2002	*The New York Times* reports on TIA's existence
12 November 2002	*The Washington Post* reports on TIA
26 November 2002	DARPA removes staff biographies from IAO mini-site
14 December 2002	*Wired* News reveals that *SF Weekly* columnist and 'culture jammer' Matt Smith has publicly disclosed Poindexter's home address and phone number
24 January 2003	US Senate votes to end DARPA's funding for TIA
7 February 2003	Under Secretary of Defense (Acquisition, Technology & Logistics) Edward C. "Pete" Aldridge Jr. conducts a Pentagon briefing on TIA to address oversight concerns. Announces the establishment of the External TIA Federal Advisory Committee. The Department of Defense releases a press release about the Committee.
11 April 2003	DARPA announces TIA's successful first tests
20 May 2003	DARPA changes TIA's name to Terrorism Information Awareness
Late 2003	DARPA ends TIA project, disbands IAO and reallocates many of the remaining R&D projects to DARPA's other R&D labs
31 December 2003	The Department of Defense's Office of the Inspector General releases a Report on TIA's oversight (12 December 2003)
2004	Bush Administration continues to invest in data-mining technologies

Bibliography

Aldridge, Jr., Edward C. 'Acquisition Programs/Total Information Awareness—Aldridge Briefs Media.' US Department of Defense briefing, March—April 2003, <http://www.findarticles.com/p/articles/mi_m0KAA/is_2_32/ai_102274043> [31 May 2006].

Anonymous. 'Total Information Awareness (TIA) Update.' US Department of Defense, 7 February 2006, <http://www.defenselink.mil/releases/2003/b02072003_bt060-03.html> [31 May 2006].

Barabasi, Albert-Laszlo. *Linked: How Everything Is Connected to Everything Else and What It Means*. Plume, New York, 2003.

Battelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. Portfolio Hardcover, New York, 2005.

Bazerman, Max H. and Watkins, Michael D. *Predictable Surprises: The Disasters You Should Have Seen Coming And How To Prevent Them*. Harvard Business School Press, Boston MA, 2004

Benjamin, Daniel and Simon, Steve. *The Next Attack: The Globalization of Jihad*. Hodder & Stoughton, London, 2005.

Berkowitz, Bruce D. and Goodman, Allan E. *Best Truth: Intelligence In The Information Age*. Yale University Press, New Haven, NJ, 2000.

Berkowitz, Bruce D. and Goodman, Allan E. *Strategic Intelligence for American National Security*. Princeton University Press, NJ, 1989.

Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. Perseus Books Group, New York, 1999.

Brooks, Fred. *The Mythical Man-Month: Essays on Software Engineering* (20th anniversary ed.). Addison-Wesley Professional, Upper Saddle River NJ, 1995.

Brown, John Seely and Duguid, Paul. *The Social Life of Information*. Harvard Business School Press, Boston MA, 2000.

Clarke, Richard A. *Against All Enemies: Inside America's War on Terror*. The Free Press, New York, 2004.

Davenport, Thomas H. and Beck, John C. *The Attention Economy: Understanding the New Currency of Business*. Harvard Business School Press, Boston MA, 2002.

Feenberg, Andrew. *Questioning Technology*. Routledge, London and New York, 1999.

Gladwell, Malcolm. *Blink: The Power of Thinking Without Thinking*. Little, Brown and Company, New York, 2005.

Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Back Bay Books, New York, 2002.

Johnson, Loch K. *Bombs Bugs Drugs and Thugs: Intelligence and America's Quest for Security*. New York University Press, New York, 2000.

Johnson, Steven. *Emergence: The Connected Lives of Ants, Brains, Cities and Software*. Scribner, New York, 2002.

Lyon, David. *Surveillance Society: Monitoring Everyday Life*. Open University Press, Buckingham PA, 2001.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy* (2nd ed.). CQ Press, Washington DC, 2005.

Mau, Bruce (Ed). *Massive Change*. Phaidon Press, London, 2004.

Nardi, Bonnie A., and O'Day, Vicki L. *Information Ecologies: Using Technology with Heart*. The MIT Press, Cambridge MA, 1999.

The National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. W.W. Norton and Company, New York, 2004.

Odom, William E. *Fixing Intelligence: For A More Secure America* (2nd ed). Yale University Press, New Haven, 2005.

Perrow, Charles. *Normal Accidents: Living With High-Risk Technologies*. Princeton University Press, Princeton NJ, 1999.

Powers, Thomas. *Intelligence Wars: American Secret History from Hitler to al-Qaeda*. New York Review Books, New York, 2002.

Poindexter, John. 'Overview of the Information Awareness Office.' DARPATech 2002, 2 August 2002, <http://www.fas.org/irp/agency/dod/poindexter.html> [31 May 2006].

Poindexter, John. 'DARPA's Initiative on Asymmetric Threat: Total Information Awareness.' DARPATech 2002, 2 August 2002, <http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/slides/PoindexterIAO.pdf> [31 May 2006].

Schneier, Bruce. *Beyond Fear: Thinking Seriously About Security In An Uncertain World*. Springer, New York, 2003.

Shulsky, Abram N and Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence* (3rd ed.). Potomac Books, 2002.

Surowiecki, James. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. Doubleday, New York, 2004.

Tenner, Edward. *Why Things Bite Back: Technology and the Revenge of Unintended Consequences*. Vintage Books, New York, 1997.

Thackara, John. *In The Bubble: Designing In A Complex World*. MIT Press, Boston MA, 2005.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information*. Cambridge University Press, Cambridge U.K., 2003.

Vaidhyanathan, Siva. *The Anarchist in the Library: How the Clash Between Freedom and Control is Hacking the Real World and Crashing the System*. Basic Books, New York, 2004.

Vise, David and Malseed, Mark. *The Google Story*. Delacorte Press, New York, 2005.

Wang, Richard; Allen, Thomas; Harris, Wesley; and Madnick, Stuart. 'An Information Product Approach For Total Information Awareness.' MIT Sloan School of Management Working Paper, https://dspace.mit.edu/handle/1721.1/1823

Weber, Steven. *The Success of Open Source*. Harvard University Press, Boston MA, 2004.

West, David. *Object Thinking*. Microsoft Press, Redmond WA, 2004.

Wurman, Richard Saul. *Information Anxiety 2*. QUE, Indianapolis IN, 2001.

[1] Defense Advanced Research Projects Agency (DARPA). 'Information Awareness Office Homepage.' The Wayback Machine, <http://web.archive.org/web/*/http://www.darpa.mil/iao/> [31 May 2006]. Anonymous. 'Information Awareness Office.' Wikipedia, <http://en.wikipedia.org/wiki/Information_Awareness_Office> [31 May 2006].

[2] Mau, Bruce (Ed). *Massive Change*. Phaidon Press, London, 2004. Thackara, John. *In The Bubble: Designing In A Complex World*. MIT Press, Boston MA, 2005.

[3] Berkowitz, Bruce D. and Goodman, Allan E. *Best Truth: Intelligence In The Information Age*. Yale University Press, New Haven, NJ, 2000. Berkowitz, Bruce D. and Goodman, Allan E. *Strategic Intelligence for American National Security*. Princeton University Press, NJ, 1989.

[4] The National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. W.W. Norton and Company, New York, 2004, p. 438.

[5] Bazerman, Max H. and Watkins, Michael D. *Predictable Surprises: The Disasters You Should Have Seen Coming And How To Prevent Them*. Harvard Business School Press, Boston MA, 2004, pp. 36—37.

[6] Coll, Steve. *Ghost Wars: The Secret History of the CIA, Afghanistan, and Bin Laden, from the Soviet Invasion to September 10, 2001*. Penguin Press, New York, 2004.

[7] Silberstein, Sandra. *War of Words: Language, Politics and 9/11*. New York: Routledge, 2002.

[8] Benjamin, Daniel and Simon, Steve. *The Next Attack: The Globalization of Jihad*. Hodder & Stoughton, London, 2005. Clarke, Richard A. *Against All Enemies: Inside America's War on Terror*. The Free Press, New York, 2004.

[9] Baer, Robert. *See No Evil: The True Story of a Ground Soldier in the CIA's War on Terrorism*. Three Rivers Press, New York, 2003.

[10] Weiss, Murray. *The Man Who Warned America: The Life And Death Of John O'Neill, The FBI's Embattled Counterterror War*. ReganBooks, New York, 2003.

[11] Odom, William E. *Fixing Intelligence: For A More Secure America* (2nd ed). Yale University Press, New York, 2004, pp. 5—6.

[12] Mayle, Adam and Knott, Alex. 'Total Business Awareness: The Corporate Contracting Behind John Poindexter's Total Information Awareness Program.' *Multinational Monitor*, vol. 24, no. 1 & 2 (January—February 2003). <http://multinationalmonitor.org/mm2003/03jan-feb/jan-feb03corp3.html> [31 May 2006]. Borin, Elliot. 'Feds Open 'Total' Tech Spy System.' *Wired* News, 7 August 2002, <http://www.wired.com/news/conflict/0,2100,54342,00.html> [31 May 2006].

[13] Aldridge, Jr., Edward C. 'Acquisition Programs/Total Information Awareness—Aldridge Briefs Media.' US Department of Defense briefing, March—April 2003, <http://www.findarticles.com/p/articles/mi_m0KAA/is_2_32/ai_102274043> [31 May 2006]. Singel, Ryan. 'Total Info System Totally Touchy.' *Wired* News, 2 December 2002, <http://www.wired.com/news/politics/0,1283,56620,00.html> [31 May 2006].

[14] Poindexter, John. 'Overview of the Information Awareness Office.' DARPATech 2002, 2 August 2002, <http://www.fas.org/irp/agency/dod/poindexter.html> [31 May 2006].

[15] The National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States*. W.W. Norton and Company, New York, 2004, p. 272.

[16] Poindexter, John. 'DARPA's Initiative on Asymmetric Threat: Total Information Awareness.' DARPATech 2002, 2 August 2002, <http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/slides/PoindexterIAO.pdf> [31 May 2006].

[17] Poindexter, John. 'DARPA's Initiative on Asymmetric Threat: Total Information Awareness.' DARPATech 2002, 2 August 2002, <http://www.darpa.mil/DARPATech2002/presentations/iao_pdf/slides/PoindexterIAO.pdf> [31 May 2006]. The sub-projects included FutureMap <http://web.archive.org/web/20021017150858/www.darpa.mil/iao/FutureMap.htm>; FutureMap Director <http://web.archive.org/web/20021003021026/http://www.darpa.mil/iao/Fosterbio.pdf>; Wargaming the Asymmetric Environment <http://web.archive.org/web/20021003045334/http://www.darpa.mil/iao/WAE.htm>; Genisys Database Querying <http://web.archive.org/web/20021017150727/www.darpa.mil/iao/Genisys.htm> and Genoa II "cognitive amplifiers" <http://web.archive.org/web/20021017152345/www.darpa.mil/iao/GenoaII.htm> [31 May 2006].

[18] Shulsky, Abram N and Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence* (3rd ed.). Potomac Books, 2002, p. 52.

[19] Wang, Richard; Allen, Thomas; Harris, Wesley; and Madnick, Stuart. 'An Information Product Approach For Total Information Awareness.' MIT Sloan School of Management Working Paper, https://dspace.mit.edu/handle/1721.1/1823

[20] Brooks, Fred. *The Mythical Man-Month: Essays on Software Engineering* (20th anniversary ed.). Addison-Wesley Professional, Upper Saddle River NJ, 1995.

[21] Schneier, Bruce. Beyond Fear: Thinking Seriously About Security In An Uncertain World. Springer, New York, 2003.

[22] Standish Group <http://www.standishgroup.com/> [31 May 2006].

[23] Feenberg, Andrew. *Questioning Technology*. Routledge, London and New York, 1999, p. 152. The model could be extended to evaluate the US Department of Justice's 'Final Independent Technical Review of the Carnivore System' <http://www.usdoj.gov/jmd/publications/carniv_final.pdf> [31 May 2006].

[24] Galloway, Alexander. *Protocol: How Control Exists After Decentralisation*. The MIT Press, 2004.

[25] Perrow, Charles. *Normal Accidents: Living With High-Risk Technologies*. Princeton University Press, Princeton NJ, 1999.

[26] Berkowitz, Bruce D. and Goodman, Allan E. *Best Truth: Intelligence In The Information Age*. Yale University Press, New Haven, NJ, 2000, p. 27.

[27] Anonymous. 'Total Information Awareness.' *The Washington Post* (16 November 2002), p. A20. < http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A61653-2002Nov15&notFound=true> [31 May 2006].

[28] Anderson, Shannon R. 'Total Information Awareness And Beyond: The Dangers of Using Data Mining Technology to Prevent Terrorism.' Bill of Rights Defense Committee, Northampton MA, 2003. <http://www.bordc.org/threats/data-mining.pdf> [31 May 2006].

[29] Scheuer, Michael [Anonymous]. *Imperial Hubris*. Brassey's, Washington DC, 2004. Scheuer, Michael [Anonymous]. *Through Our Enemies' Eyes: Osama Bin Laden, Radical Islam and the Future of America*. Brassey's, Washington DC, 2002. Stern, Jessica. *Terror in the Name of God: Why Religious Militants Kill*. Ecco Books, New York, 2004.

[30] Shulsky, Abram N and Schmitt, Gary J. *Silent Warfare: Understanding the World of Intelligence* (3rd ed.). Ibid, pp. 64, 142, 162.

[31] Berkowitz, Bruce D. and Goodman, Allan E. *Best Truth: Intelligence In The Information Age*, Ibid, pp. 116—117.

[32] Nardi, Bonnie A., and O'Day, Vicki L. *Information Ecologies: Using Technology with Heart*. The MIT Press, Cambridge MA, 1999.

[33] Spiller, Neil (Ed.). *Critical Writings for the Digital Era*. Phaidon Press Limited, London, 2002. Waldrop, M. Mitchell. *The Dream Machine: J.C.R. Licklider and the Revolution that Made Computing Personal*. Penguin, New York, 2002. Bardini, Thierry. *Bootstrapping: Douglas Engelbart, Coevolution, and the Origins of Personal Computing*. Stanford University Press, 2000.

[34] Brown, John Seely and Duguid, Paul. *The Social Life of Information*. Harvard Business School Press, Boston MA, 2000. Davenport, Thomas H. and Beck, John C. *The Attention Economy: Understanding the New Currency of Business*. Harvard Business School Press, Boston MA, 2002.

[35] Gladwell, Malcolm. *Blink: The Power of Thinking Without Thinking*. Little, Brown and Company, New York, 2005. Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Back Bay Books, New York, 2002. Surowiecki, James. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. Doubleday, New York, 2004.

[36] Markoff, John. 'Pentagon Plans a Computer System That Would Peek at Personal Data of Americans.' *The New York Times* (9 November 2002), <http://www.nytimes.com/2002/11/09/politics/09COMP.html> [31 May 2006]. O'Harrow, Jr., Robert. 'U.S. Hopes To Check Computers Globally.' *The Washington Post*, 12 November 2002, <http://www.washingtonpost.com/ac2/wp-dyn/A40942-2002Nov11> [31 May 2006]. Anonymous. 'Military Intelligence System Draws Controversy.' CNN, 20 November 2006, <http://archives.cnn.com/2002/US/11/20/terror.tracking/> [31 May 2006].

[37] Levin, Jonathan. 'Total Preparedness.' *The National Review* (13 February 2003), <http://www.nationalreview.com/comment/comment-levin021303.asp> [31 May 2006].

[38] Healy, Gene. 'Beware of Total Information Awareness.' 20 January 2003, <http://www.cato.org/dailys/01-20-03.html> [31 May 2006].

[39] Scardaville, Michael. 'No Orwellian Scheme Behind DARPA's Total Information Awareness Program.' The Heritage Foundation, 20 November 2002, <http://www.heritage.org/Research/HomelandDefense/wm175.cfm> [31 May 2006]. McCullagh, Declan. 'George Orwell, Here We Come', C|Net, 6 January 2003, <http://news.com.com/George+Orwell,+here+we+come/2010-1071_3-979276.htm> [31 May 2006].

[40] American Civil Liberties Union Spying Center <http://www.aclu.org/privacy/spying/> [31 May 2006]. Anonymous. 'Total Information Awareness.' Human Rights First <http://www.humanrightsfirst.org/us_law/privacy/tia.htm> [31 May 2006].

[41] Ramasastry, Anita. 'Why We Should Be Concerned About 'Total Information Awareness' And Other Anti-Terrorism Strategies For The Internet.' FindLaw, 31 December 2002, <http://writ.news.findlaw.com/ramasastry/20021231.html> [31 May 2006].

[42] Barlow, John Perry. 'John Perry Barlow on the Total Information Awareness Program.' *TalkLeft*, 8 February 2003, <http://talkleft.com/new_archives/001707.html> [31 May 2006].

[43] Boyd, Stowe. 'Social Networking = Volunteer 'Total Information Awareness'.' 7 January 2004, <http://www.corante.com/getreal/archives/2004/01/07/social_networking_volunteer_total_information_awareness.php> [31 May 2006].

[44] Rheingold, Howard. 'Congress Nixes Total Information Awareness.' *Smart Mobs*, 13 February 2003, <http://www.smartmobs.com/archive/2003/02/13/congress_nixes_.html> [31 May 2006].

[45] Kick, Russ. 'Information Awareness Office Website Deletes Its Logo.' *The Memory Hole*, 2002, <http://www.thememoryhole.org/policestate/iao-logo.htm> [31 May 2006]. Fiore, Mark. 'Total Information Awareness.' *San Francisco Chronicle*, 28 May 2003, <http://www.sfgate.com/cgi-bin/article.cgi?file=/gate/archive/2003/05/28/fioretia2.DTL> [31 May 2006]. Dupree, Chuck. 'Total

Information Awareness, Redux.' *Bad Attitudes*, 27 November 2003. <http://badattitudes.com/MT/archives/003375.html> [31 May 2006).

[46] Dunn, Andy. 'The Other Domestic Spying.' *Z Magazine* (March 2006), <http://zmagsite.zmag.org/Mar2006/dunn0306.html> [31 May 2006].

[47] Belasco, Amy. 'Total Information Awareness Programs: Funding, Composition, and Oversight Issues', Congressional Research Service (21 March 2003), <http://www.au.af.mil/au/awc/awcgate/crs/rl31786.pdf> [31 May 2006].

[48] A brief survey of TIA archives would include ComputerBytesMan <http://www.computerbytesman.com/tia/>; EPIC's TIA Page <http://www.epic.org/privacy/profiling/tia/> and Briefing <http://www.epic.org/events/tia_briefing/>; the EFF's TIA Page <http://www.eff.org/Privacy/TIA/>; Iwar <http://www.iwar.org.uk/news-archive/tia/total-information-awareness.htm>; Cryptome <http://cryptome.org/tia-queeg.htm>; GeoCities <http://www.geocities.com/totalinformationawareness/>; Missouri University <http://foi.missouri.edu/totalinfoaware/>; 7Gen <http://7gen.com/topics/politics/total-information-awareness>; Lumpen
TIA Links <http://www.lumpen.com/world/surveillance.html> [31 May 2006].

[49] Schor. Daniel. 'Poindexter Redux.' *The Christian Science Monitor*, 29 November 2002, <http://www.csmonitor.com/2002/1129/p11s01-coop.html> [31 May 2006]. Schor, Daniel. 'Total Information Awareness.' *NPR*, 18 November 2002, <http://www.npr.org/templates/story/story.php?storyId=846795> [31 May 2006].

[50] Barnes, Peter. 'Tracking John Poindexter.' 20 December 2002, <http://www.techtv.com/news/news/story/0,24195,3412114,00.html> [31 May 2006].

[51] Newitz, Annalee. 'Totalitarian Information Awareness.' *AlterNet*, 27 November 2002, < http://www.alternet.org/story/14656/> [31 May 2006].

[52] Boutin, Paul. 'Keeping Track of John Poindexter.' *Wired* News, 14 December 2002, <http://www.wired.com/news/politics/0,1283,56860,00.html> [31 May 2006].

[53] Hertzberg, Hendrik. 'Too Much Information.' *The New Yorker* (9 December 2002), <http://www.newyorker.com/talk/content/?021209ta_talk_hertzberg> [31 May 2006].

[54] Lewis, Charles. 'Total Information Awareness: A Chance Encounter Raises Questions.' Center for Public Integrity, 17 December 2002, <http://www.publicintegrity.org/report.aspx?aid=107&sid=200> [31 May 2006].

[55] Carney, David. 'DoD Releases Report on DARPA's Total Information Awareness Program.' *Tech Law Journal*, 31 December 2003, <http://www.techlawjournal.com/topstories/2003/20031231.asp> [31 May 2006]. Anonymous. 'Information Technology Management: Terrorism Information Awareness Program (D-2004-033).' Office of the Inspector General, Department of Defense, Arlington VA, 2003 <http://www.dodig.osd.mil/audit/reports/FY04/04-033.pdf> [31 May 2006].

[56] Battelle, John. *The Search: How Google and Its Rivals Rewrote the Rules of Business and Transformed Our Culture*. Portfolio Hardcover, New York, 2005. Vise, David and Malseed, Mark. *The Google Story*. Delacorte Press, New York, 2005.

[57] Brin, David. *The Transparent Society: Will Technology Force Us to Choose Between Privacy and Freedom*. Perseus Books Group, New York, 1999. Regan, Tom. 'US Still Funding Powerful Data-Mining Tools.' *The Christian Science Monitor*, 23 February 2004, <http://www.csmonitor.com/2004/0223/dailyUpdate.html> [31 May 2006].

[58] Moore, Geoffrey A. *Crossing the Chasm: Marketing and Selling Products to Mainstream Customers* (rev. ed). HarperBusiness, New York, 2001.

[59] Anonymous. 'Whistle-Blower's Evidence, Uncut.' *Wired* News, 22 May 2006, <http://www.wired.com/news/technology/0,70944-0.html?tw=wn_index_23> [31 May 2006]. Hansen, Eric. 'Why We Published The AT&T Docs.' *Wired* News, 22 May 2006, <http://www.wired.com/news/technology/0,70947-0.html?tw=wn_index_24> [31 May 2006].

[60] Georgia10. 'Did Hayden Break The Law?' *The Daily Kos*, 13 May 2006, <http://www.dailykos.com/tag/Total%20Information%20Awareness> [31 May 2006].

[61] Schaffer, Eric. *Institutionalization of Usability: A Step-By-Step Guide*. Addison-Wesley, 2004.

[62] West, David. *Object Thinking*. Microsoft Press, Redmond WA, 2004, pp. 185—200.

[63] Berkowitz, Bruce D. and Goodman, Allan E. *Strategic Intelligence for American National Security*, Ibid, pp. 195—202.