UNISCI Discussion Papers

THE U.S. INTELLIGENCE REFORM AND THE NATIONAL INTELLIGENCE STRATEGY OF OCTOBER 2005

AUTHOR:[1]

GUSTAVO DÍAZ
UNISCI / University of Salford

Introduction

Efforts to improve, alter, or reorganise the U.S Intelligence community are as old as the U.S. intelligence community itself. The terrorist attacks in 2001 brought renewed calls for intelligence reform, with some of the most persistent advocates arguing, "if not now, when. It is important to remember that as Mark M. Lowenthal defends "intelligence is a government activity, where revolutionary proposals tend to be ignored"[2]. What is certain is that the debate over U.S. intelligence reform will go on, largely on its own momentum, with heightened attention during crises or after incidents deemed to be intelligence failures. There have been recent changes to the U.S. intelligence community since 9/11. One of them has been the addition of another agency to the monstrosity that is the bureaucracy of the intelligence community, which is composed of 15 intelligence agencies at present, including those within the State, Defence, Homeland Security, Treasure, Energy, and Justice (counterintelligence) Departments.

So far efforts at reform have been either too difficult to manage or too politically charged to be acceptable. Further, efforts at reform have almost always been triggered by perceptions of failure or hints of scandal. Typically, the response to either scandal or failure has been to look for ways to reorganise the system rather then seek to change the way it works[3]. One of the major problems affecting the discussions about reform of the U.S Intelligence Community is the absence of a commonly understood and accepted doctrine. Since the publication of the National Intelligence Strategy, there are internal standard procedures but no clearly articulated doctrine. Senior officials usually spend careers within a single agency, and therefore they arrive in senior posts largely ignorant of other parts of the intelligence Community. Without a doctrine for intelligence, they have tended to defend the parochial resources interest of their home agencies[4].

---

[1] *Las opiniones expresadas en estos artículos son propias de sus autores. Estos artículos no reflejan necesariamente la opinión de UNISCI.* The views expressed in these articles are those of the authors. These articles do not necessarily reflect the views of UNISCI.

[2] Lowenthal, Mark (2003): *Intelligence: From Secrets to Policy.* Washington D.C.,Westport, p. 232.

[3] Hulnick, Arthur S. (1999): *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First centur.* Westport, Praeger, p. 191.

[4] Odom, William E. (2003): *Fixing Intelligence, For a More Secure America*, New York, Yale University Press, p. 11.

William E. Odom pointed out "Do serious structural and organisational problems really exist? One does not need access to classified information to answer yes. It would be extraordinarily surprising if there were not"[5]. Since the U.S. Intelligence Community structure settled into place some forty years ago, it has remained essentially unchanged. Meanwhile, technologies have advanced at a blinding pace in the following decades. The communications revolution alone provides grounds for suspecting that major structural reforms in the Intelligence Community are long overdue. Some adaptations have been made, but not enough to allow full exploitation of the technologies. In that sense, structural problems afflict not only intelligence collection but also intelligence analysis. The needs of executive branch policy-makers, for whom this intelligence was primarily produced, tended to be secondary in both agencies calculations. For example, the handling of intelligence analysis on al Qaeda in the weeks and days leading up to the events of 11 September 2001 offers another example of problems in both analysis and distribution of intelligence[6]. As William E. Odom has recently said "critical scrutiny of the U.S. intelligence community is clearly justified, scrutiny of its structure, organisation and management arrangements"[7] .

1. The historical precedents of U.S. Intelligence reform

Since the Congress of the US began investigating the Intelligence Community in the mid-1970s, the issue of intelligence reform has been raised repeatedly. During the Carter administration several initiatives were taken to implement some of the ideas produced by a committee chaired by Senator Frank Church (D-Idaho), but no fundamental structural change occurred. Several times in the1980s congressional oversight committees raised the reform issue, and David Boren (D-Okla) actually drafted legislation for several structural changes in the US intelligence community. The House committee also offered an alternative draft, but neither bill became law. In 1994 Senator John Warner (R-Va) introduced legislation for a presidential commission to consider Intelligence Community reforms, and his bill became law. The resulting commission produced its report in early 1996[8]. At the same time, several unofficial intelligence reform studies produce a flurry of activity and a wide variety of proposals[9] were submitted.

Most of the reform efforts were inspired by sensational problems and episodes within the Intelligence Community, especially in the Central Intelligence Agency (CIA). The church committee was outraged by the evidence that the CIA had attempted assassinations as part of covet actions in the past, and that the army's counterintelligence units had been used to help the Federal Bureau of Investigation (FBI) keep track of antiwar movement leaders in the late 1960s and early 1970s. On the other hand in the late 1980s, CIA covert actions in Central America became the focus of renewed interest in intelligence reform. In the 1990s a number of incidents within the CIA, involving serious operational failures and still others involving

[5] *Ibid.,* p. 4
[6] *Ibid.*, p. 5
[7] *Ibid,* p. 7
[8] Presidential Commission on the Roles and Capabilities of the United States Intelligence Community (1996): "The Aspin Brown Commission", *Preparing for the 21st Century: An Appraisal of U.S Intelligence.* Washington: U.S. Government Printing Office.
[9] See *Making Intelligence Smarter: The future of U.S Intelligence,* New York, Council on Foreign Relations; *The Future of U.S Intelligence,* Washington, Consortium for the Study of Intelligence (1996); *In front the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S Intelligence,* New York, Twentieth Century Fund Press (1996).

National Reconnaissance Office accountability for funds, brought the issue once again to congressional and public attention.

After almost three decades of such episodes, no fundamental reform has occurred in the U.S. Intelligence community. Virtually all congressional investigations and reform studies have merely focused on the scandals and raised policy issues. With few exceptions[10], however, structural reform has been largely ignored.

2. The U.S. Intelligence community in the 21st Century

Over the past twenty years, western intelligence services have had to adjust themselves to a succession of radical changes. The world of the 21st century is likely to be fraught with new dangers, coupled with more uncertainty and unpredictability than at any other time in history[11]. The international arena has became more complicated with the multiplication of actors, sources of crises, means of conflict, increasing economic interdependence, accelerating technological developments and the growing interconnectivity of information and communications; therefore new dynamics and vulnerabilities are now present.

These realities make assessments more complex, developments less predictable and crises and conflicts less calculable. In a field where a great deal of emphasis is placed on reducing uncertainty[12], it is a necessity to remodel the intelligence services for the new requirements of the 21st Century. The information revolution is not just about cheaper communications or faster computers. The information revolution is also changing how people use information to which they have access[13]. To adapt, the intelligence community must abandon many of the old principles on which it was based, replacing them with new approaches. Finally, we must also recognise though that globalization and the technological revolution will provide limited benefits for intelligence services. For this century's new threats, technology by itself will be of no use. Terrorist groups operate in small networks and may therefore avoid being picked up by technical intelligence methods.

As President Bush has declared, "...in an age in which we are at war, the consequences of underestimating a threat could be tens of thousands of innocent lives." He continued: "and my administration will continue to make intelligence reforms that will allow us to identify threats before they fully emerge so we can take effective action to protect the American people."[14]

Consequently, it can be argued that human intelligence will be fundamental for this new century. Today's intelligence services are constrained by national budgets and congressional controls; therefore it will be fundamental that governments redefine the role of intelligence

[10] For example, one major feature of the Boren bill of the late 1980s, was the creation of the National Imagery Agency or the creation of the National Imagery and Mapping Agency on 1 October 1996.
[11] Gannon, John C.: "The role of Intelligence Services in a globalised world", 21 May 2001, in http://www.cia.gov/nic/speeche_globalizedworld.html.
[12] Lowenthal, Mark M. (1992): *U.S Intelligence: Evolution &Anatomy,* Westport, Praeger, p. 19.
9 Treverton, Gregory F. (2001): *Reshaping National Intelligence for an Age of Information*. Cambridge, Cambridge University Press, p. 21.
[13] Berkowitz Bruce D. y Goodman Allan E. (2000): *Intelligence in the Information Age.* New Haven / London, Yale University Press.
[14] President Bush, George W.: *America's Intelligence Capabilities and Weapons of Mass Destruction*, Dwight D. Eisenhower Executive Office Building, Washington, DC, 31 March 2005, in http://www.state.gov/nea/rls/rm/44068.htm.

with the adoption of networked and more flexible structures, thereby making them more efficient. The set of tasks for intelligence services in the 21st century are more complex, more volatile and more numerous than during the cold war. The ethos for tasking intelligence services has always been to go after that which cannot be acquired better, more safely or more cheaply by any other means. The methods of collection have changed dramatically and for the 21st century intelligence services must adapt to the new international environment.

Intelligence is understood both as "information" (such as in the case of the Cuban Missile Crisis) and as instrument of policy (such as in the role of Intelligence in Iraq in 2003), so intelligence is a function of a set of national security objectives and tasks. In this sense intelligence must be something that helps the policy-makers to decide among competing options or that can be used as an instrument they can wield in their relations with foreign powers. The only propose of the intelligence product for the policy-makers is to serve and assists in the formulation and execution of national security policy, because we cannot forget that intelligence is necessary but not a sufficient requirement for effective national security policy. But for the decision-makers intelligence is also a function of policy in a second less understood sense, one that is usually neglected in public discussions of the intelligence policy nexus. Intelligence activities, process and organisations can be used to implement national security policy and to achieve political objectives. In other words, decision-makers have their own expectations about what intelligence can do for them and have both the right and the duty to choose how to meet their needs. How the decision-makers choose to be served by intelligence can determine how intelligence information is acquired and the intelligence activities undertaken serve them in setting and executing national security policy.

Today in the dawn of the 21st century the policy-makers have to prioritise targets. The information available will always exceed somewhat our capacity to collect and process, in that sense the policy-makers must be conscious of the new requirements for the new century. In the coming century, a great deal of low-intensity conflict and political warfare is likely to take place, "active measures" and covert action, because terrorism is likely to consume most of the policy-makers time and energy. Moreover, such threats are relatively more intelligence-intensive than other aspects of national security policy. Furthermore, they tend to require more human intelligence and specialised, highly targeted, technical collection. Prediction is one of the qualitative measures of intelligence, and it is usually reserved for major political and military events. There have been different authors who point out that the 20th Century may be seen as the age of secret intelligence, because the main focus of intelligence was on penetrating secrets and protecting secrets.

The 21st century, by contrast, may be the age of public intelligence[15]. In that sense Tony Blair revealed a Joint Intelligence assessment about Iraq saying in its preface "It is unprecedented for the government to publish this kind of document"[16]. Considering that intelligence has been practised in its different forms since the dawn of time it seems paradoxical that it has only been 'an academic discipline for half a century.' The conceptual framework in which intelligence is studied must continue evolving and adapting to the new conditions and possibilities of the early 21st century. As more intelligence and intelligence related material than ever before enters into the public domain, scholars of international relations must take greater account of it and study of the role of intelligence.

[15] The idea of public intelligence was found in Wark, Wesley K.: "Learning to Live with Intelligence", *Intelligence and National Security,* Vol. 18, No. 4, (2003). Also see: Tenet, George J., Director of Central Intelligence: "Iraq and Weapons of Mass Destruction", Georgetown University, 5 February 2004, in http://www.cia.gov/cia/public_affairs/speeches/2004/tenet_georgetownspeech_02052004.html

[16] Tenet, *op. cit.,* p. 6.

The Freedom of Information Act (FOIA)[17], which was signed into law by President Lyndon B. Johnson on July 1966, established public access to government information in the U.S Information not exempted from public disclosure was deemed available to virtually anyone regardless of nationality. Laws were passed requiring that U.S. government agencies release their records to the public on request[18]. While 9/11 was the presumed catalyst for the revamped FOIA guidelines, the policy change was actually in keeping with Bush's historic aversion to the release of government papers. In this sense under the Bush administration, the information available has been insignificant[19], including many aspects of National Security. Following the September 11th terrorist attacks, the Bush Administration passed the Oct. 12.2001 Directive to federal agencies to purge a wide array of potentially sensitive data from their web sites, a decree that, for a time, removed the entire online presence of the Nuclear Regulatory Commission, and which ultimately resulted in hundreds of thousands of pages being deleted from sites maintained by the Department of Energy, the Environmental Protection Agency, the National Archives and Records Administration, and other federal entities. On March 25, 2003, President George W. Bush signed an order that postponed, by three years, the release of millions of twenty-five-year-old documents slated for automatic declassification the following month. What is more, Executive Order 13292, which amended a Clinton Administration order, granted FOIA officers wider powers to reclassify information that had already been declassified and further eliminated a provision that instructed them not to classify information if there was "significant doubt" about the need to do so.

In November, President George W. Bush signed Executive Order 13233, "Further Implementation of the Presidential Records Act", to restrict access to historical presidential papers. Notwithstanding of the measures after 9/11, the cuts in the freedom of information under Bush Administration are a step back to the correct understanding of the requirements of secrecy in a democratic society to protect the National Security, and not to increase the power of the state. As Intelligence deals with information it has been greatly affected by the "information age". The effects of these changes show in several different ways. At one level, they suggest new ways in which information can be more rapidly circulated and used, but not only for the government; society has also been affected by increasing information availability.

However, as Bruce Berkowitz suggests "intelligence is not a 'necessary evil' that democracies must engage in. Intelligence policies are not fundamentally different from other kinds of policies, and intelligence operations are not inherently different from other kinds of operations democracies carry out"[20]. Nowadays more than ever, intelligence is not only about

[17] *The Freedom of Information Act,* in http://www.foia.cia.gov.

[18] A vast bulk of information controlled by the federal government was made available under the act, but many exceptions are applied. These include classified national defence and foreign policy information, privileged or confidential trade and financial information, internal personnel records and documents, information concerning certain law enforcement matters, and geological and geophysical research information concerning wells. FOIA presents serious problems for its application. If it is true that "anyone" can apply for a FOIA, the waiting time is substantial, as any discretionary decision to disclose information protected under the FOIA should be made only after full and deliberate consideration of the institutional, commercial, and personal privacy interests that could be implicated by disclosure of the information. But we cannot forget that the process is very expensive, "The Justice Department says a group that wants to see secret documents about the detention of people jailed after the Sept. 11 attacks first must pay nearly $373,000 to cover the cost of searching for the information". See: "U.S demands pay for records search", *Chicago Tribune,* 1 February 2005, in http://www.chicagotribune.com. The advance payment doesn't guarantee anything found will be released, and in many cases the trouble is not worth it.

[19] Smith, R. Jeffrey: *Washington Post*, 1 March 2005, p. A02.

[20] http://www-hoover.stanford.edu/publications/digest/031/berkowitz.html.

secrets. Secrecy is an important element of intelligence, but as Sherman Kent has indicated, intelligence is about information and knowledge that is vital to national survival[21].

3. 9/11 as an intelligence failure

As the events of 11 September have once again forced intelligence issues onto agenda, the initial reactions have been to treat them primarily as policy matters, ignoring the underlying structural issues. One of the main questions for intelligence in this regard is: Could better intelligence have actually stopped the 9/11 hijackers? The 9/11 Commission certainly believed it could, and this led to the passage of new legislation supposedly designed to make sure that the intelligence problems associated with 9/11 are fixed. In hindsight, as the 9/11 Report correctly points out, detecting the terrorist plot should have been possible if only the "dots" had been connected.

In a field where a great deal of emphasis is placed on reducing uncertainty[22], it would be somewhat disheartening to accept that failures may be inevitable, yet the possibility of failure is an inherent aspect of intelligence[23]. Failure in intelligence has always attracted more attention than success. Writers on strategic surprise have examined the failure of intelligence services to prevent a wide variety of unexpected events that pose a threat to national security; post 9/11[24] the study of intelligence failure has become of particular national concern in the U.S. Despite the traditional focus of intelligence failures being on the analytical process, today it is fundamental to face new threats with effective collection in vast networks. In discussing the new threats, one of the main problems is the collection of information rather than the analysis of them.

These "new" threats are very much diverse; therefore greater emphasis must be placed on identifying an adversary's intentions rather than its capabilities. It is of greater difficulty to assess the intentions of a terrorist group rather than its capabilities. Although there may be strategic indicators of terrorist threats one would expect to see fewer tactical intelligence indicators of terrorist attacks. The first few years of the 21st century have witnessed a transformation in the role of secret intelligence in international affairs. Intelligence and security issues are now more prominent than ever before, in Western political discourse as well as the wider public consciousness.

Public expectations of intelligence have never been greater. As Christopher Andrew points out "during only a year, the threats posed by Osama Bin Laden and Saddam Hussein had succeeded in transforming British government on the public use of intelligence"[25]. The relationship between policy makers and their intelligence advisors come under unprecedented public scrutiny in the United Kingdom and also the U.S. The leaders of both countries were charged with purposefully distorting intelligence information in order to justify their decisions to declare war in Iraq in April 2003.

[21] Kent, Sherman (1949): *Strategic Intelligence for American World Policy*. Princeton, Princeton University Press, p. vii.
[22] Lowenthal, *op. cit,* p.19.
[23] Betts, Richard: "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable", *World Politics,* Vol. 31, No. 1 (1978), p. 62
[24] Goodman, Melvin: "9/11.The failure of strategic Intelligence", *Intelligence and National Security*, Vol. 8, No. 4 (Winter 2003), p. 59-71.
[25] Andrew, Christopher: "Intelligence, international relations and under theorization", *Intelligence and National Security,* Vol. 19, No. 2 (Summer 2004), pp. 29-30.

The 9/11 Commission, in its report issued in July 2004, found that the intelligence community suffered from a lack of institutional imagination before the 11th September 2001 attacks on New York City and Washington. Chapter 8 of the Report goes into great detail about how the Intelligence Community did not fully understand the warning signs, even though ''the system was blinking red'' with them in the summer of 2001. Chapter 11 describes the many missed opportunities to disrupt al-Qaeda operations. The Community had critical information at its disposal, but it could not sense the importance of what it was seeing. Still, none of the 9/11 Commission proposals offers a clear suggestion about how to institutionalise imagination.

Encouraging the use of alternative analysis was one of the more useful recommendations that emerged from the report issued in March 2005 by the team of former Judge Laurence Silberman and former Virginia Governor and Senator Charles Robb.[26] The 600-page report, which denounced the intelligence system for its failure to analyse correctly the allegation that Saddam Hussein had weapons of mass destruction in Iraq, was yet another blow to an intelligence system trying to reorganise in the wake of the 9/11 attack. Some of the changes suggested by Silberman and Robb had already been started when their report appeared; others were dismissed as hard to accomplish. For example, calling for more spies on the ground is easy for such a study commission, but hard to manage, especially in situations where the intelligence officers involved would be serving under the kinds of nonofficial cover that might leave them vulnerable to arrest and possible abuse by local security services.

The 9/11 Commission recommended declassifying intelligence spending, which is currently hidden in the defence budget. It correctly argued that no informed public debate over priorities can occur as long as the public is kept unaware of the total spending and basic distribution of funds in the Intelligence Community. This proposal was both sensible and long overdue. Unfortunately, Congress did not include it in the final reform package.[27]

The Commission also proposed the creation of an expanded National Counter-terrorism Centre (NCTC), as well as a number of smaller issue specific analytic centres. This recommendation was included as part of the Intelligence Reform and Terrorism Prevention Act of 2004. Modelled after the military's combatant commands, these ''national intelligence centres'' are to focus on specific issues and regions. The 9/11 Commission recognises that the issues are less technical than policy related in nature. In that sense, the primary purpose of the centres is to help policy-makers coordinate information by pooling intelligence and streamlining information channels. President George W. Bush quickly announced his support of the 9/11 Commission's recommendations when they were made public in July 2004, issuing in August 2004, three executive orders.

Executive Order (EO) 13354[28] established the National Counter-terrorism Centre under the direction of the Director of Central Intelligence (DCI) to integrate U.S. intelligence on terrorism and counter terrorism, conduct strategic operational planning for counter- terrorism activities, assign and coordinate responsibilities for such actions, serve as the central knowledge bank on terrorist groups, and ensure information sharing.

[26] Report of the Commission on the Intelligence Capabilities of the U.S. *Regarding Weapons of Mass Destruction*, 31 March 2005, in http://www.wmd.gov.
[27] 9/11 Commission Report, p. 416.
[28] Executive Order 13354 of 27 August 2004, "National Counterterrorism Centre", in http://www.fas.org/irp/offdocs/eo/eo-13354.htm

EO 13355[29], billed as a measure to strengthen the DCI's authority in managing the Intelligence Community, actually reaffirmed previous orders directing specific intelligence agency heads to give the now defunct position of Director of Central Intelligence (DCI) access to their information and assist him in developing the National Foreign Intelligence Program (NFIP) budget and keep intact the Defence Secretary's operational control over the major defence intelligence agencies and intelligence priorities. This was no different from previous practice, where the DCI developed collection and analysis priorities in response to National Security Council (NSC) guidance, even though interagency committees, working through the DCI's Community Management Staff and the Assistant DCI for Collection, actually sorted out the priorities, which were then implemented by the core agencies of the Intelligence Community,Central Intelligence Agency (CIA), National Security Agency (NSA), National Reconnaissance Office (NRO), and National Geospatial Agency (NGA). With close inspection of he executive order, the conclusion must be that the only new material in its guidance to the DCI to develop objectives that would be consistent with the intelligence priorities enunciated in National Security Presidential Directive (NSPD), issued in 2003.

Finally, EO 13356[30] directed all agencies working on terrorism and counter-terrorism issues to cooperate in collecting intelligence, producing intelligence reports, sharing such intelligence freely with one another, and disseminating such intelligence widely throughout the Intelligence Community. The executive order established an Information Systems Council (ISC) to develop and operate interoperable terrorism information sharing systems, and required the sharing of terrorism information free of the originator-controlled (ORCON)[31] limitation, a stipulation that surely produced consternation in the CIA, which has to date been the principal user of the ORCON designation. Despite of these, as Helen Fessenden argues "There is still no single office or individual in the intelligence community to mandate information sharing across all agencies"[32].

4. USA Patriot Act

After 9/11 The "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act" of October 2001, better known by its acronym: "USA PATRIOT ACT"[33], decreased the ability of American citizens to obtain information about their government and, at the same time, gave the government the means to pry into the personal lives of those same citizens[34]. In essence, the Patriot Act authorised a

[29] Executive Order 13355 of August 27, 2004, "Strengthened Management of the Intelligence Community", in http://www.fas.org/irp/offdocs/eo/eo-13355.htm

[30] Executive Order 13356 of August 27, 2004, "Strengthening the Sharing of Terrorism Information To Protect Americans", in http://www.fas.org/irp/offdocs/eo/eo-13356.htm.

[31] When an agency disseminates intelligence and other classified information, it must ensure that only the appropriate people receive the information. Specifically, the recipients of classified information must have a need to know the information and have been granted the proper level of security clearance. The agency that originally collected the intelligence may mark it ORCON, or originator controlled. All agencies that receive this information must receive permission from the originating agency before further dissemination. Agencies usually mark a document ORCON for two reasons. First, it allows the originating agency to protect the sources and methods disclosed in the classified document. Second, it is a vehicle to allow the originating agency to control how the information or conclusions in a document are used.

[32] Fessenden, Helen: "The Limits of the Intelligence Reform", *Foreign Affairs,* Vol. 84, No. 6 (2005), p. 118

[33] *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*, in http://www.fas.org/irp/crs/RL31377.pdf.

[34] Milchen, Jeff: "Patriot Act II Bush Administration Escalates Its War on Americans", *Freedom Pacific New Services*, 11 February 2003, in http://news.pacificnews.org/news.

host of new law enforcement and intelligence-gathering provisions sought by Attorney General John Ashcroft and the Bush Administration. For example, the Act includes changes to the laws regulating surveillance, making it easier for the government to surreptitiously gather information about individuals[35]. This law dismantles the regulatory firewall between internal and external intelligence, which was erected in the late 1970s in the wake of the Watergate investigations of intelligence abuses. In fact the CIA and the FBI are now much more free to share information.

5. The concept of public intelligence

In September 2002 Tony Blair's government issued a 55 page dossier on Iraq´s weapons of mass destruction, the first published official document based on detailed Joint Intelligence committee (JIC) assessments. Tony Blair said in his introduction that "It is unprecedented for the government to publish this kind of document"[36].Tony Blair finally rested the traditional taboo that the British government does not mention their intelligence services. Officially the secret services did not even exist. We can argue that after September 11 the threats posed by Osama Bin Laden and Saddam Hussein had succeeded in transforming British government policy on the public use of intelligence. Today intelligence is more deeply and visibly embedded in the conduct of international relations than ever, over a whole range of issues from counter-terrorism to UN peacekeeping.

Also in September 2002 the Bush administration in the National Security Strategy[37] pointed out the necessity of good intelligence after the cold war and the appearance of the "new threats" of the 21st century, "In a new environment in which a fusion might occur between the new age's worst nightmares, terrorism, rogue states and the proliferation of weapons of Mass Destruction…". The document laid down three conditions for the future performance of intelligence[38]: Firstly, the requirement for good intelligence and early warning of emerging threats. Secondly, the need to build international coalitions on the basis of a shared conviction about emerging threats. Finally, the capacity to win pre-emptive wars quickly, with minimal causalities.

The last war in Iraq was the first test case for the strategy of pre-emption. In 16 October 2003, in San Bernardino, California, Bush reiterated American determination to pursue a strategy of preemption, when circumstances demanded it. The challenge for America, as Bush put it, was to "show our motives are pure"[39]. And as Wesley K. Wark describes them, "pure motives" require public intelligence[40]:

> We conclude that, if intelligence is to be used more widely by governments in public debate in future, those doing so must be careful to explain its uses and limitations. It will be

[35] Schulhofer, Stephen (2002): *The Enemy Within: A Century Foundation Report.* New York, The Century Foundation Press, p. 1.
[36] *Iraq's Weapons of Mass Destruction: The Assessment of the British Government*. London, The Stationery Office, 24 September 2002.
[37] http://www.whitehouse.gov/nsc/nss.html.
[38] Wark, Wesley: "Learning to live with Intelligence", *Intelligence and National Security,* Vol. 18, No. 4 (2003)
[39] http://www.whitehouse.gov/news/releases/2003/10/20031016-3.html
[40] *Ibid.,* p. 126.

essential, too, that clearer and more effective dividing lines between assessment and advocacy are established when doing so[41].

It could be said that the age of public Intelligence will demand a revolutionary change in the practice of intelligence and the doctrine of secrecy; but we cannot forget that great care will also be required in protecting intelligence sources and methods, to ensure that the intelligence product does not become completely politicised. Intelligence is always important for the decision making and as Christopher Andrew and David Dilks reminded us "intelligence is the missing dimension in our understanding of critical policy-making decisions in the realm of international relations".

The pre-emptive attack is now official U.S. policy. With such doctrine, the role of intelligence has become fundamental. With this in mind, the case for a pre-emptive attack based on Iraq's weapons of mass destruction capability was backed by the intelligence community[42]. According to Bob Woodward in his book *Plan of Attack*, "The underlying intelligence about the threat from another country, the power and quality of information, was a point worth discussing, Rumsfeld believed. What information would you require and with what degree of certainty before you launched a pre-emptive attack?"[43]

As Richard A. Best defends "Despite the importance of intelligence, the evidence collected and analysed by U.S. intelligence agencies in recent years may not have been the central factor in framing U.S. policies towards Iraq"[44]. Some senior policy-makers in the Bush Administration had come into office with a deep conviction that Saddam Hussein's government presented an ongoing threat to U.S. and Western interests in the Middle East.

In particular, the pre-war intelligence estimate that Iraq was reconstituting an extensive nuclear program was largely discredited[45]. However, policies will be judged on their results. Intelligence analysis can inform policymaking, but it does not substitute for it[46].

Except for the disagreement on reconstruction of Iraq's nuclear program, intelligence solidly backed the Bush administration, when they began to argue for military action against Iraq. The U.S. intelligence community was in agreement regarding Iraq having a biological and chemical weapons capability. Unfortunately, this knowledge was based on reliable information in most cases at least 15 years old and, in the best case, over five years old. In fact, no one in the U.S. intelligence community had valid information confirming that Iraq possessed weapons of mass destruction. In that sense, there is a crucial difference between knowing and assuming. The issue of a link between Iraq and terrorism was more divisive, not within the intelligence community, but between the intelligence community and those in leadership positions. The solution, the policy employees recommended, was to ignore the CIA

[41] *Butler Committee Report,* in http://www.archive2.official-documents.co.uk/document/deps/hc/hc898/898.pdf, p. 146.
[42] U.S. Senate Select Committee on Intelligence (SSCI): "Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq", 7 July 2004, p. 461, in http://www.intelligence.senate.gov/iraqreport2.pdf.
[43] Woodward, Bob (2004): *Plan of Attack.* New York, Simon and Schuster, p. 133.
[44] Best, Richard A. Jr. "U.S. Intelligence and Policymaking: The Iraq Experience", *CRS Report for Congress,* 2 December 2005, http://fpc.state.gov/documents/organization/32000.pdf, 6 January 2006.
[45] See *Statement by David Kay on the Interim Progress Report on the Activities of the Iraq Survey Group (ISG)*, 2 October 2003, en http://www.odci.gov/cia/public_affairs/speeches/2003/david_kay_10022003.html. The Report adds, however, that "We have discovered dozens of WMD-related program activities and significant amounts of equipment that Iraq concealed from the United Nations during the inspections that began in late 2002."
[46] Best, *op. cit.*

analysis of the reliability of the sources and just take the raw information at face value. "we know the answers; give us the intelligence to support the answers"[47]. In fact, the question of an Al-Qaeda link with Iraq was investigated by the 9/11 Commission[48]. Unfortunately for the Bush administration, there was no evidence upon which the intelligence community could assess that there was a formalised link between Iraq and Al- Qaeda. There were reports of some meetings, and even of some individual training, but no evidence of an ongoing Iraq-Al-Qaeda connection[49].

The Senate Committee on Intelligence conducted a review of pre-Iraq War Intelligence and issued a report on 7 July 2004. The committee looked into allegations of "pressure" applied by policy-makers on intelligence analysis to change their assessments. The overall committee report stated in its conclusions that "The committee did not find any evidence that administration officials attempted to coerce, influence or pressure analysts to change their judgments related to Iraq's Weapons of Mass Destruction capabilities"[50]. In fact, intelligence supporting a pre-emptive attack against Iraq was shaped, from the top down, by the leaders of the Bush administration. The intelligence assessment that there were no formal ties between al-Qaeda and Iraq was correct, but was not accepted by the Bush administration. Lacking the answer they sought from the intelligence community, the administration turned to an ad hoc team in the Department of Defence.

The senate select of committee on intelligence took up the challenge to determine how intelligence had reached its erroneous conclusions long before David Kay came to his revelation. In June of 2003 the Committee reviews of the Pre-War intelligence on Iraq. Nearly a year later the Committee released the first part of his findings of the 7th July 2004. The Bipartisan Committee agreed to 1017 conclusions, the first being: "most of the major key judgment in the intelligence community's October 2002 National Intelligence Estimate (NIE), *Iraq's continuing programs for weapons of mass destruction, either overstated or where not supported by the underline intelligence reporting. A series of failures, particularly in analytic trade craft, let to the mischaracterization of the intelligence.*[51]

The Committee limits "group thinking" to the intelligence community only and stresses in its conclusions that there was no political pressure on analysts to change their assessments. Several members of the Committee disagree about the absence of political pressure.[52] When it came to weapons of mass destruction there was little need for pressure, everyone from the President down believed that Saddam possessed weapons of mass destruction. When conducting a pre-emptive war, the evidence of eminent danger should be clear. Secretary of Defense Rumsfeld believed, according to Woodward's *Plan of Attack,* that the Intelligence upon which a pre-emptive attack was based, should be vetted.[53] The Bush administration, however, admitted that they did not need, nor could they afford, to wait for a smoking gun in the form of a mushroom cloud.[54] The objectivity of intelligence was hindered by a leadership that only questioned assumptions that were contrary to the administration "group think".

[47] As General William C. Westmoreland said related to the war in Vietnam in June 1968. Sharp, U.S.G. and Westmoreland, William C. (1968): "Report on the War in Vietnam". Washington, GPO, p. 199.
[48] "The 9/11Commission Report", pp. 228-229, in http://www.9-11commision.gov/report/911report.pdf. (Accessed 14 September 2005).
[49] U.S. Senate Select Committee on Intelligence (SSCI), *op. cit.,* pp. 345-348.
[50] *Ibid.,* p. 284.
[51] U.S. Senate Select Committee on Intelligence, "Report on the US Intelligence...", *op. cit.,* p. 14.
[52] *Ibid.,* pp. 449, 457-459, 500-501.
[53] Woodward, *op. cit.,* p. 133.
[54] *Ibid.,* pp. 179, 202.

Objectivity was further clouded by the dual responsibilities of the Director of Central Intelligence to implement policy through covert operations, while at the same time providing analysis that could potentially contradict that same policy.

Leaders make decisions and have an intense commitment to the success of their policy, according to Deputy Secretary of Defense Paul Wolfowitz in an article on the relationship of intelligence and policy-makers.[55] If intelligence challenges the assumptions of policy, Wolfowitz suggests that intelligence must emphasise the evidence, laying out the facts and their relationships. The analysts must also be prepared to defend their positions. While the intelligence community apparently maintained its objectivity regarding the link between Al-Qaeda and Saddam Hussein, it fell victim to a cumulative loss of objectivity and "group thinking" regarding Iraq's weapons of mass destruction. There is little doubt there is a conflict of interest and loss of objectivity when intelligence crosses over into the realm of implementing policy through analysis without facts. The Senate Select Committee on Intelligence criticised the Central Intelligence Agency for not having a single spy with knowledge of Iraq's Weapons of mass destruction.[56] In fact, all the technical capability of the United States intelligence community proved inadequate in proving information on Iraq's weapons of mass destruction and ties with Al- Qaeda.

As Richard Perle pointed out "Since the attacks on the World Trade Centre and the Pentagon, terrorism has become the first priority of the U.S. government"… "President Bush's war on terror jerked our national security bureaucracy out of its comfortable routines. He demanded that the military "fight new wars in new ways"[57]. This ideology meant that with Iraq, U.S. forces overthrew Saddam Hussein's entire regime with half the troops and in half the time it previously took to merely shove Saddam out of Kuwait in 1991.However, at the same time the U.S is losing the peace[58]. It cannot be forgotten although, that when it is accepted that the first line of defence against terrorism has to be better intelligence, the perceived integrity of the intelligence agencies should not have been undermined, by the distortion of the reports in the course of the political process. For the Bush administration it was just a matter of time before Saddam Hussein would regain the resources to acquire the weapons of Mass Destruction that he tried to develop in the past.

President Bush and Prime Minister Blair "must" make judgements on the best available evidence, and they must weight the evidence carefully, always mindful of the consequences of acting under conditions of uncertainty derivate of the nature of the intelligence itself. For Richard Perle, "a failure to act on the available intelligence by taking the risk that Saddam did not possess weapons of mass destruction and therefore leaving him in place could have catastrophic consequences. But the dangers to remove him would entail far less risk, far less danger, than discovering too late that he did indeed have the chemical and biological weapons"[59].

At the same time the Bush administration described the threat posed by Saddam´s regime as "global", that is for all countries, not only the U.S. Although, from my point of view, it is

[55] Davis, Jake: "The Challenge of Managing Uncertainty: Paul Wolfowitz on Intelligence-Policy Relations", *Studies in Intelligence,* Vol. 39, No. 5 (1996), in http://www.cia.gov/csi/studies/96unclass/davis.htm. (Accessed 15 September 2005).
[56] U.S. Senate Select Committee on Intelligence, "Report on the US Intelligence...", *op. cit.,* p. 260.
[57] Frum, David and Perle, Richard (2003): *An End to Evil: How to Win the War on Terror.* New York, Random House, pp. 5-7.
[58] Boot, Max: "The New American Way of War", *Foreign Affairs* (July- August 2003), p. 43.
[59] Frum and Perle, *op. cit.*, p. 26.

now clear that the U.S. and Britain did not find the right balance of persuasion and objectivity in their public analyses of the threat before the war and in their arguments in favour of the conflict. Further more, no evidence surfaced during or soon after the war that tracked with the previous U.S. and British intelligence assessments, indicating that Iraq had the capability to use weapons of mass destruction in war fighting, or indicated had active programs for the production of weapons mass destruction that were creating an imminent threat.

6. The creation of the "Director of National Intelligence" (DNI)

It is enormously difficult to make different agencies in the huge national security bureaucracy to work together. President Bush has issued an executive order calling on U.S. intelligence agencies to share information related to terrorism and set up an "Information Sharing Council." The 9/11 Commission called for a National Intelligence Director (NID), while the final legislation designated a Director of National Intelligence (DNI). For the sake of clarity we use only the latter title.[60] The legislation also included provisions that direct the DNI to use high-quality analytic all methods, and to protect the objectivity of analysis. However, the DNI's real authority is ambiguous. The creation of the new post of Director of National Intelligence, or DNI, in an effort to coordinate the 15 different federal agencies engaged in intelligence work.

Despite Congress rush to pass the legislation, the White House quickly discovered that finding someone with the proper credentials to take the DNI job was not so straight forward. Several well-known officials decided to pass up the position, including Army General Tommy Franks, who knew little about the inner workings of intelligence, and former Director of Central Intelligence (DCI) Robert M. Gates, who perhaps knew too much[61]. Finally, in early 2005, President George W. Bush named John Negroponte, a career diplomat and former ambassador to the United Nations (UN) and Iraq, as his first DNI. New DNI John Negroponte, must assert his authority over the agencies, which the legislation leaves somewhat vague. In the words of Arthur S. Hulnick "the DNI position was not given the kinds of control over the IC that were necessary. The legislation was ambiguous at best, and seems to be causing more harm than good[62]".

Although given broad nominal control over budgets, personnel, and tasking, there is no guarantee that the DNI, John Negroponte, will have the bureaucratic influence to impose his will over the community, especially because the reform bill stated that the DNI cannot "abrogate the statutory responsibilities"' of the Secretary of Defense. Meanwhile, DCI Porter A. Goss will fight to retain control over the CIA after being stripped of other responsibilities. Under these conditions, how the DNI will be able to force the Community to become more imaginative is itself hard to imagine. The DNI "shall establish a process and assign an individual or entity the responsibility for ensuring that, as appropriate, elements of the intelligence community conduct alternative analysis… of the information and conclusions in intelligence products."

Traditionally in the U.S. intelligence community there is not a single individual in charge of everything. The 1947 Act known as the National Security Act, named the Director of the

[60] "The 9/11Commission Report", *op. cit.*, p. 428.
[61] Hulnick, Arthur S.: "Indications and Warning for Homeland Security: Seeking a New Paradigm", *International Journal of Intelligence and Counterintelligence*, 18 (2005), p. 7
[62] *Ibid*, p. 9

Central Intelligence (DCI) as the primary advisor of intelligence issues[63]. But the creation of the Director of National Intelligence replaces the DCI as the 1st advisor to the president. The problem is that the DNI does not have a collection agency or a bureaucratic basis, but despite of this they have a lot of budget power. As Helen Fessenden concludes, "Negroponte's office is simply another layer of bureaucracy over all agencies rather than a force that can push through necessary structural changes to streamline the intelligence community and foster more accountability"[64]. In this sense Negroponte has significant power on paper, but he has spent much energy on projects that do little to further bureaucratic transformation. The new (DNI) will not have a free hand to dramatically reshape American intelligence, for example, by collapsing all the intelligence collectors into a single agency.

7. The National Intelligence Strategy, October 2005

The new concept of "national intelligence" codified by Intelligence reform and the terrorist prevention act was passed by congress in 2004. Its publication on October 26, 2005 coincided with the six-month anniversary of the establishment of the Office of the Director of National Intelligence (ODNI). A comprehensive U.S. strategy that was designed to integrate the missions of the 15 intelligence agencies better, while enhancing the collection of intelligence on threats to U.S. national security world-wide was released by the director of national intelligence. As John Negroponte affirms "national intelligence must be collaborative, penetrating, objective and far sighted"[65]. In other words, the Strategy is a strengthening and solidification of the existing Homeland/National Security apparatus into a more centralised structure.

The document sets forth the framework for a more unified, coordinated and effective Intelligence Community trying to address the main changes occurring in the world today for the intelligence services, as John Negroponte points out: "a strategy is statement of fundamental values, highest priorities, and orientation toward future, but it is an action document as well. For the US national Intelligence, the time for change is now. There are no easy answers to the risks contemplated here or the risks that might come"[66].

> The National Intelligence Strategy will guide Intelligence Community policy, planning, collection, analysis, operations, programming, acquisition, budgeting, and execution. These activities will be overseen by the ODNI, but implemented through an integrated Intelligence Community. Outlining the document's two types of strategic objectives, mission and enterprise, the strategy recognises each Intelligence Community member's strengths and competencies.

As detailed in the strategy, mission objectives relate to those efforts to predict, penetrate, and pre-empt threats to the U.S. national security, and assist all who make and implement U.S. national security policy, fight U.S. wars, and enforce the laws.

Missions objectives outlined in the National Intelligence Strategy are as follows[67]:

---

[63] With the new legislation it is not clear who is going to give the president the daily brief among other issues.
[64] Hulnick, Arthur S., *op. cit.,* p. 119.
[65] *The National Intelligence Strategy for the United States of America* (October 2005), *in* http://www.globalsecurity.org/intell/library/policy/national/nis-usa_october2005.pdf
[66] *Ibid.*
[67] *Ibid.*

1. *Defeat "terrorists" at home*[68] *and abroad by disarming their operational capabilities and seizing the initiative from them by promoting the growth of freedom and democracy.* Nowadays, terrorism is a traditional threat with a new face, due to the impact of globalisation and new technologies. Today global terrorism[69] has different aspirations than the ideological terrorism of the twentieth century. This new kind of terrorism is at war against western values and it wishes to destroy the western way of life. Intelligence rather than military or police force has been the first line of prevention against this kind of threat. Terrorism presents many problems for the intelligence services[70], as they are often closely networked groups. This being the case we must emphasise human intelligence as fundamental in the war against terror. Intelligence will also need new approaches[71] in meeting terrorist threats, as the old structures of the cold war are inappropriate for this new kind of "war".

2. *Prevent and counter the spread of WMDs*. The spread of advanced conventional and unconventional military technologies, (chemical, biological, and nuclear), as well as the ballistic missiles to deliver them; is creating new instabilities.[72] Those who possess unconventional weapons may be tempted to use them. Those who do not possess them, or those who see themselves as especially vulnerable to unconventional warfare, may be tempted to act against these capabilities before they can be fully deployed or employed by adversaries. Thus, there is not only a diffusion of political power, but a corresponding diffusion of military power that has greater potential for devastation if order breaks down[73]. We must not forget the importance of controlling weapons of mass destruction, conventional arsenals, small arms proliferation, sensitive technologies and their relationship both to rogue state threats and global terrorism[74]. Both present a common characteristic in that they are willing to utilise such weapons for tactical success. Intelligence will be essential in meeting such a threat by controlling and monitoring the movement of double-use materials and the movement of weapons around the world.

3. *Bolster growth of democracy. This includes the "support of diplomatic and military efforts (including pre-and post-conflict) where intervention is necessary"*. In this particular regard, the **assumption that democratic nations are peaceful countries** is rooted in the post-World War II reconstruction of West Germany and Japan, because the two former members of the Axis were transformed from America's mortal enemies into close allies and trading partners. As President George W. Bush put it: "because democracies respect their own people and their neighbours, the advance of freedom will lead to peace." Although there may be a certain amount of truth to this logic, it is not necessarily true that all future democracies will be friendly to the United States, especially democracies in Muslim countries. If free and popular elections were held in Pakistan, Egypt, Saudi Arabia and Jordan, the resulting governments would likely be anti-American.

---

[68] Note the emphasis on "at home".

[69] Kurth Cronin, Audrey: "Behind the curve .Globalization and International Terrorism", *International Security,* Vol. 27, No. 3 (Winter 2002/03), p. 42.

[70] Aid, Matthew M: "All Glory is Fleeting: Signit and the fight against international terrorism", *Intelligence and National Security,* Vol. 18, No. 4 (Winter 2003), p. 81

[71] Herman, Michael, "Counter-Terrorism, Information Technology and Intelligence Change"*, Intelligence and National Security,* Vol. 18, No.4 (Winter 2003), p. 42.

[72] Haass, Richard N. (1999*): Intervention: The Use of American Military Force in the Post-Cold War World.* Washington, DC, Brookings Institution, p. 71.

[73] Scott, James A. (1998): *After the End: Making U.S. Foreign Policy in the Post-Cold War World*. Durham, NC, Duke University Press, p. 74

[74] *National Strategy to Combat Weapons of Mass Destruction* (December 2002), in http://www.whitwhouse.gov/news/releases/2002/12/wmdstrategy.pdf.

4. *Develop innovative ways to penetrate and analyses the most difficult targets (the unnamed "targets" are characterised as "tough adversaries that know a great deal about our intelligence system").* There is a relative weakening of the nation-state. Technology, the Internet, television, telephones and fax machines all increase the scope and impact of communications across state borders, making it much more difficult for governments to control what their citizens know and what others know about them. Moreover, the state is getting weakened from the outside (regional organizations, a stronger UN Security Council, International Monetary Fund, non-governmental organisations, corporations, and private individuals)[75]. These trends contribute to the difficulty and at times inability of existing governments to contend with challenges to their authority.

5. Anticipate developments of "strategic concern". The world of the 21st century is likely to be fraught with new perils, coupled with more uncertainty and unpredictability than at any other time in history[76]. The international arena has became more complicated with the multiplication of actors, sources of crises, means of conflict, increasing economic interdependence, accelerating technological developments and the growing inter-connectivity of information and communications; therefore new dynamics and vulnerabilities have come into play.

The U.S. Intelligence Community must provide the basis of knowledge for a state; they must also, at all times, be able to warn of impending crises and detect possible surprises, dangers, threats or attacks in advance. The principal mission of an intelligence service is to alert and support decision makers (political or military) on issues with which they are concerned. The rapid evolution of the strategic, political and economic environment since the end of the Cold War has furthered the quest for information on security issues that governments will have to pursue. With conventional military threats diminishing[77], new risks and dangers connected with proliferation, globalisation and destabilisation multiply the security challenges. These realities make assessments more complex, developments less predictable and crises and conflicts less calculable. In a field where a great deal of emphasis is placed on reducing uncertainty[78], it must be necessary to remodel the intelligence services for the new requirements of the 21st Century.

Enterprise objectives relate to the ability to transform faster than threats emerge, protect what needs to be protected, and perform U.S. duties according to the law. Enterprise objectives in The National Intelligence Strategy are[79]:

1.-*Build an integrated intelligence capability to address threats to the homeland, consistent with U.S. laws and the protection of privacy and civil liberties.* With the fall of the Soviet Union the nature of conflict has changed. Today there are many non-military risks and threats, and the development of internal conflict and failed states requires new approaches for intelligence services. Cooperation and intelligence sharing will be fundamental for the success of international coalitions.

2.-*Strengthen analytical expertise, methods, and practices; tap expertise wherever it resides; and, explore alternative analytical views. 3.- Rebalance, integrate, and optimise*

[75] Scott, *op. cit.* p. 60
[76] Gannon, *op. cit.*
[77] For the end of the Cold War and how we explain later on for the different changes in the nature of the conflict.
[78] Lowenthal, *op. cit.*, p. 19. Also see Treverton, *op. cit.*, p. 21.
[79] *The National Intelligence Strategy, op. cit.*

collection capabilities to meet current and future customer and analytic al priorities. In this sense monitoring the activities and intentions of Islamic extremists has proven exceptionally difficult due in part to their vastly diverse backgrounds.

4.-Attract, engage, and unify an innovative and results-focused Intelligence Community workforce. 5.-Ensure that Intelligence Community members and customers can access the intelligence they need when they need it. Which means a great focus in the U.S. intelligence cycle as a tool to respond to the threats of the 21st Century century.

6.-*Establish new and strengthen existing foreign intelligence relationships to help the U.S. meet global security challenges.* At the end of the Cold War many of the traditional intelligence alliances of these democratic states were downgraded and in some cases broken off.[80] The lack of a common enemy meant that interests diverged and with it the close co-operation of intelligence services. A great deal of emphasis was placed on economic intelligence as the greatest priority for nation-states.[81] With the developing threat of asymmetric warfare from authoritarian states and Islamic extremists, these intelligence services have had to readjust to new realities. By the end of the 20th century the intelligence services of these liberal democratic states had begun to recognise the importance of co-operation in dealing with the threat of weapons of mass destruction (WMD) and the authoritarian states seeking to utilise them.[82] With the increasing number of terrorist attacks by Islamic extremists, intelligence alliances will be crucial in dealing with the two major threats of the 21st century. As intelligence services spent much of the last century being preoccupied with symmetrical warfare, they will also have to make structural adjustments in order to combat the rise of trans-national asymmetric threats.

7.-*Create clear, uniform security practices and rules that allow the U.S to work together, protect secrets, and enable aggressive counterintelligence activities.*

8.-*Exploit path-breaking scientific and research advances that will enable the U.S to maintain and extend our intelligence advantages against emerging threats.* In this sense, the American intelligence agencies must move faster, further, and in more directions than once thought possible, in order to just keep up. Similar challenges face any other country's intelligence establishment. Coming at a time of renewed crisis and conflict, with major decisions on the horizon concerning the commitment of intelligence resources, these challenges are clear, stark, and unavoidable.

9.-*Learn from successes and mistakes to anticipate and be ready for new challenges.* Intelligence has to be used as evidence for the decision-making, not as interference. In Iraq, for example, the WMD were not found by the time the decision had to be made. In that sense, most analysts inside and outside the U.S. government including those who opposed going to war would have bet that Iraq still had WMD programs and some stockpiles, at least of chemical weapons. That's why U.S intelligence needs to focus even harder on improving collection and on understanding the true limits of information at any given moment. Even the best analyst cannot make intelligence out of whole cloth. But the most important lesson to

[80] Pollack, Kenneth M.: "Securing the Persian Gulf: Washington Must Manage Both External Aggression and Internal Instability", *Brookings Review* (Fall 2003), p. 21.
[81] Danker, John: "Economic Espionage Increases, Threatening National Security", *Insight on the News*, 18 July 1994, p. 38.
[82] Deutch , John M. and Smith, Jeffrey H.: "Smarter Intelligence", *Foreign Policy* (January-February 2002), p. 67.

draw from the war in Iraq is appreciating how intelligence really fits into the making of U.S. foreign policy.

Attempting to understand an often-hostile world with incomplete data is, in essence, not an intelligence problem at all. Indeed, it's a policy problem, and pivots on the kinds of risks an official is willing to accept on behalf of his country. Critics of the Bush administration claim officials "cherry picked" intelligence to fit their own preconceptions or relied too much on outside analysts. This suggests that intelligence is or ought to be the most important input for government officials. In reality, intelligence is just one drop in a fire-hose torrent of facts and analysis a decision-maker sees every day. Personal contacts, think tank papers, press reports, and the gut reactions that the decision-maker brings to office are usually much more important. After all, that's why we have elections. If policy automatically followed from intelligence, what would be the sense in choosing one candidate over another? When used prudently, intelligence can contribute to good policy. But history shows that any policymaker can seize upon bits of intelligence that confirm his or her worst fears or greatest hopes, especially when there's little to choose from. Even as that data begins to look more fragile, those long-cherished views can be hard to let go. That's exactly how policy and intelligence should work in a democracy.

On the other hand the UK, the main vehicle for the Government's use of intelligence in the public presentation of policy was the dossier of September 2002[83]. The assessment of Iraqi WMD capabilities served as the prime justification for a succession of decisions and actions that led to the invasion of Iraq in March, 2003. This justification for the war has come under acute scrutiny because of the apparent failure to locate the expected stockpiles of WMDs. On 14 July, Lord Butler of Brockwell derived his report on the intelligence that contributed to the decision to go to war in Iraq[84]. It will have to do with the future working of the British intelligence services and their relationship with the Government, rather than the government presentation of intelligence product to a public audience.

Lord Hutton cleared the Government of deliberately inserting false intelligence into their published dossier on Iraqi WMD. The Hutton Report left the wider questions about the Government's propriety in its handling of intelligence unanswered. For instance, questions remain regarding the possibility that the Government and Intelligence Services "cherrypicked" intelligence that tended to support the case for war, and/or that the public presentation of this intelligence was misleading. One of the main conclusions of the Inquiry was that key intelligence used to justify the war with Iraq has been shown to be unreliable. Examining the management of British intelligence in the light of evidence presented to the Butler Inquiry it showed clearly that the failure to find WMD in Iraq six months after Saddam was toppled was 'a failure of intelligence, not of Government'. Prime Minister, Tony Blair, had not been guilty of inventing intelligence, as had been alleged, to support a policy decision (to attack Iraq)[85]. If the intelligence community is found entirely at fault, then critics of the government will conclude that the intelligence community has been made a scapegoat.

In trying to diagnose any failure of intelligence it is essential to bear in mind that intelligence is not about whether or not one **has complete information**; the purpose of intelligence is to acquire fragments of information where otherwise there would be none. One rarely, if ever, has all of the pieces of the proverbial jigsaw puzzle. It is evident that the raw

[83] "Iraq's Weapons of Mass Destruction: The Assessment of the British Government", in http://www.fco.gov.uk/Files/kfile/iraqdossier.pdf.
[84] "Butler Committee Report", in http://www.butlerreview.org.uk/report/index.asp.
[85] *Ibid*., p. 119.

intelligence available was highly fragmentary, and of limited reliability. In intelligence terms the raw intelligence was accurate, or as accurate as possible, but it was erroneously assessed by the members of the Joint Intelligence Committee. In this scenario, those responsible for evaluating, collating and integrating intelligence with information from other open sources, reach incorrect conclusions either by basing the assessment on false assumptions about the intelligence target, or by incorrectly weighting or interpreting the available intelligence. Much of what the intelligence indicated was that the Iraqi regime was still pursuing research programmes in chemical and biological weapons, and had a nuclear research programme on paper but held in abeyance until a lifting or loosening of sanctions allowed its reactivation.

Respecting this particular point, I strongly think that Saddam was not an imminent threat to the West. He may have had weapons but I think he had no means of delivery. More important, he had no motive: no ideological dispute with the West and he was not suicidal. In my view, material was cooked up to try to provide a rationale for the Prime Minister's decision to back Bush in the Iraq invasion. For the decision-makers, the only propose intelligence's product serves is to assist in the formulation and execution of national security policy. But intelligence is not sufficient requirement for effective national security policy. Decision-makers have their own expectations about what intelligence can do for them. In that way how policy-makers choose to be served by intelligence can determined how intelligence information is acquired and the intelligence activities as well. however, policy-makers have devoted little effort to understanding the role of intelligence in the formulation and execution of national security policy.

10.-*Eliminate redundancy and programs that add little or no value and re-direct savings to existing and emerging national security priorities.*

Conclusion

There had been an assumption that the end of the Cold War would usher in a period of international relations in which political and military competition would diminish and the need to use force abroad would decline[86]. By the beginning of the 1990s, it looked as though a world was emerging in which democratic and market-oriented governments would dominate, in which long festering conflicts were being solved, and in which the United Nations was finally beginning to resemble the institution desired by its founders.[87] The Soviet Union and later Russia were working with the U.S. to manage conflicts; gone were the days when Russia provided material and diplomatic backing for its client states while casting vetoes in the Security Council to frustrate Western initiatives. Neither Russia nor anyone else was able or willing to compete with the U.S. as a superpower in the political-military realm on a global scale. It thus became possible for the George H.W. Bush administration to speak of building a new world order in which states did not threaten or use force to settle disputes and governments embraced democracy, human rights, and liberal economic policies[88].

In reality things have developed very differently to this view. There have been some positive developments, including movement toward rapprochement in the Middle East, as

[86] Snow, Donald M. (1991): *The Shape of the Future: The Post-Cold War World*, Armonk, NY: M.E. Sharpe, p. 16
[87] Scott, *op. cit*., p. 14.
[88] O'Hanlon, Michael E. (1992): *The Art of War in the Age of Peace: U.S. Military Posture for the Post-Cold War World*, Westport, CT, Praeger, p. 32.

well as peace and prosperity in Latin America and East Asia. But there are many undesirable developments, including a variety of humanitarian disasters in Africa, growing tensions on the Korean Peninsula, several civil wars, the threat of WMD proliferation, and lastly terrorism. On balance, the post-Cold War world has been a messy one where violence is common, where conflicts within and between nation-states are common, and where the question of military intervention becomes more, rather than less important, and more, rather than less complicated.

The changes intrinsic to the post-Cold War world have created new, intense conflicts that complicate any prospective use of force. On the other hand, a number of political and technological developments enhance opportunities to use military might effectively. The erosion of blocs and alliances makes it easier (in the political sense) to use force against individual states.[89] There is little fear of direct conflict between superpowers growing out of a local confrontation with a third state, and less danger that a great power rival will furnish political, economic, and military support to client states.

Modern wars have revealed emerging technologies, in particular precision-guided munitions (PGMs), creating new, more discrete opportunities for countries to act militarily.[90] Far fewer munitions can be used with equal or greater impact.[91] The chance of unwanted (collateral) damage is less. Other technologies provide greater confidence of access to the airspace of another country at lower levels of vulnerability. Improvements in other areas (from communications to intelligence) can enhance opportunities to use force effectively on modern battlefields.

Today's political environment is significantly different and, in important ways, more complex. All this creates opportunities for, and places special pressures and constraints on diplomacy and intelligence. Liberated from the danger that military action will lead to confrontation between superpowers, western alliances are now freer to intervene. Traditionally, a foreign policy driven by inter-state relations emphasises such considerations as the non-use of military force to settle disputes, opposition to the acquisition of territory by force, and respect for state sovereignty. The goal is peace, both for its own sake and because peace is likely to promote the evolution of an international context more supportive of a free flow of goods and services. Moreover, a world at peace and involved in productive commerce is more likely to produce liberal political structures than a world at war militarily and economically.[92] Moreover, only the United States possesses the means to intervene decisively in many situations, in particular those that are more demanding militarily. Yet U.S. means are limited; there will always be more interests to protect than resources to protect them. The United States can do anything, but not everything. There remains a need to choose whether to intervene.

Despite considerable discussion to the contrary, the Intelligence Reform and Terrorism Prevention Act of 2004, passed in December of that year, does not significantly alter the U.S. Intelligence Community. Over the short term, some necessary but therefore politically unpalatable corrective measures will give the appearance of significant change. But the opportunity for comprehensive intelligence reform has come and gone, and centrifugal forces within and outside the Intelligence Community—those who favour ‘‘stovepiping’’ and keeping intelligence agencies at each other’s throats— have shown themselves politically

[89] Scott, James A , *op. cit*., p. 81.
[90] Weiss, Thomas G. (1991): *Third World Security in the Post-Cold War Era.* Boulder, CO, Lynne Rienner, p. 166.
[91] *Ibid.,* p.167.
[92] Cimbala, Stephen J. (1996): *Clinton and Post-Cold War Defence*. New York, Praeger, p. 78.

stronger than centripetal forces of consolidation and greater unity of command. As Helen Fessenden points out ""as any legislation, the success of the intelligence bill depends largely on its implementation. But in this case, the political momentum to build on initial gains is running out of steam just at the critical point"[93].

The U.S. Intelligence community identity has included provisions for keeping U.S. intelligence divided and its management weak for fear that doing otherwise might lead to a rogue intelligence apparatus bent on trampling on American democracy and civil liberties. This intelligence identity, in turn, has enabled the intelligence agencies to entrench themselves in America's political culture, and to engage in the bureaucratic politics of interagency competition for turf, money, people, and access to policy-makers, actions the wider political culture viewed as necessary to prevent intelligence from getting too much power[94].

In the same sense, The National Intelligence Strategy of the U.S. changes nothing about what really matters, because it is almost entirely focused on Counter-terrorism and WMD issues. There is little attention paid to improving important military intelligence requirements like reform of the national and defence Indications and Warning systems. The significance of the National Intelligence Strategy is not the nuts and bolts of how to make the intelligence community better. Rather, it is the larger strategic context of what the intelligence community is supposed to accomplish: "provide accurate and timely intelligence and conduct intelligence programs and activities directed by the president," build better, more integrated intelligence capabilities to provide timely, accurate information on threats, wherever they may emerge.

A structured bureaucratic monster has been created. The existing U.S. intelligence Community within the U.S. comprises of fifteen different agencies, with a reported total budget of 35–40 billion dollars, a sum that is both staggering and stupefying. Many of its individual component agencies are far larger than the entire national intelligence services of most foreign countries[95]. Financial resources are huge, especially for those offices most directly involved in the global war on terrorism. Trying to describe ''U.S. intelligence'' is like trying to describe an entire ecosystem. To imagine a unified, cohesive ''Intelligence Community'' in the first place, with all agencies sharing the same world outlook and marching to the same beat, is a little misleading. More accurate, instead, is a confederation of organisations that may or may not cooperate, or that may or may not agree on specific issues at any one time. The astounding size and mind-bending complexity of the U.S. intelligence family make it more appropriate to envision an amalgamation of powerful sovereign agencies, coalitions, factions, and interest groups. The discussion here concentrates largely on three of the national-level agencies, CIA, NSA, and the Defence Intelligence Agency (DIA). While "information sharing" has become fundamental in the war on terror, existing procedures, with each intelligence agency controlling the information it produces, makes it hard enough to share within U.S. intelligence, let alone pass information to state and local authorities. The intelligence culture of secrecy is dangerously out of date. That culture is designed to protect information, not share it, which ultimately frustrates almost all reform ideas and efforts. Analysis of terrorist threats, for instance, would be improved by consulting people who have *no* "need to know" but bring a different perspective and might see patterns the ostensible experts do not.

[93] Fessenden, *op. cit.*, p. 108.
[94] *Ibid*, 113.
[95] Treverton, *op. cit.*, pp. 167–176.

With liberal-democracy becoming the normative form of governance globally, asymmetric threats have been evaluated and analysed from the perspective of a liberal-democratic alliance. Whilst terrorism will in essence be waged asymmetrically, it is the threat of weapons of mass destruction from bellicose authoritarian states that will increase the likelihood of this form of warfare being utilised in furthering state interests. New scientific and technological developments have allowed authoritarian states and Islamic extremists to benefit from increasingly fluid trans-national flows, thus increasing the likelihood of WMD capabilities being acquired, and aiding in the organisation and co-ordination of attacks. Trans-national threats will therefore require trans-national intelligence alliances.

The intelligence services of liberal-democratic states will have to strengthen their estimative and human intelligence capabilities in order to be self-sufficient in meeting these threats. Steering clear of intelligence alliances with non-democratic states may not only lead to a favourable public response, but also reduce the likelihood of 'blowback'. Avoiding the intelligence pitfalls of short-term thinking, will allow these agencies to utilise covert action as it should be used; as part of the long-term strategic interests of a state[96]. Democracies rarely if ever pose a national security threat to states with similar forms of governance; therefore the use of intelligence within this context will be fulfilling the strategic interests of all liberal-democratic states for the 21st century and beyond. The principal role of intelligence in meeting the threats of the 21st century will be to be prepared for anything and everything.

[96] Berkowitz, Bruce D. and Goodman, Allan E.: "The Logic of Covert Action", *The National Interest,* No. 51 (Spring 1998).