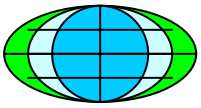
IAS Reader **Strategy Paper 1-2010**

Friedrich W. Korkisch

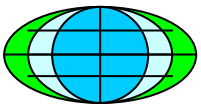
NATO Gets Better Intelligence

New Challenges Require New Answers to Satisfy Intelligence Needs for Headquarters and Deployed/Employed Forces

Vienna, Updated April 2010



IAS
INSTITUT FÜR AUSSEN- UND SICHERHEITSPOLITIK
Center for Foreign and Defense Policy



IAS

Friedrich W. Korkisch: PhD (summa cum laude) in International Relations; Col. Ret. (Air Force, Air Staff/MoD: Aerial Warfare and Space Affairs, International Air Operations, 1972-2002; lecturer Government Strategic Leadership Course since 2004 (ongoing); Member of the Austrian Delegation to the CSCS/OSCE, OSCC, Vienna, (Ministry of Foreign Affairs) and Military Adviser to the OSCC (1991-2002); Member Science Board of the MoD, and Chairman Strategic and Security Policy Advisory Commission, MoD; (since 2007); Director Center for Foreign and Security Policy, Vienna; University of Vienna (Magister, Political Science, Economic Theory, International Law, 1981-1984); Board of Europäisches Forum Alpbach; Santa Barbara City College, CA; University of Michigan, Zrinyi Milkos Univ. Budapest; Alumni NESA/National Defense University, Washington DC; International Studies Association, University of Arizona, Tucson, AZ; Lecturer of Corvinus Univ., Budapest.

Content

Introduction

Originally, this article was based on a verbal invitation by SHAPE in 2004 to look somewhat deeper into NATO intelligence. The rather critical outcome of the first draft was mirrored in the title *NATO Needs Better Intelligence*. In the meantime certain corrections were implemented.

Over the years, NATO had identified some weak areas and implemented a number of improvements. One was the *Fusion Center*, others were lessons learned in the aftermath of the terrorist attacks of September 11, 2001, lessons learned in Iraq and Afghanistan, by the Australians in East Timor, errors made in the operations that Israel had waged against southern Lebanon 2006 and the Gaza Strip in 2009, the use of UAVs for intelligence gathering and counter-strikes, recent Special Forces raids into Pakistan and in the Philippines, and improving the C4ISR/C4ISTAR and Net-Centric Warfare capabilities.

Events and proposals were analyzed, formalized and introduced, but without changing standardized procedures too much. When Afghanistan emerged again as a growing trouble spot in the fall of 2006, intelligence saw a chance to show the difference that good and timely intelligence could made. Still there were a number of intelligence failures, mainly based on some clumsy procedures, but the J2/A2/G2/CIA/DIA and air reconnaissance establishment tried to fulfill expectations and even more. But at the same time were intelligence officers criticizing the established ways intelligence was requested, formalized, ordered, handled, conducted and processed. All the high quality and speed won by better communication was lost by political and hierarchical obstacles and more and more commands which wanted to be involved in the process.

Today, much of the intelligence reporting is routinely sent to highest levels of government and the military establishment. Political judgment followed the political imperative of *success* and *progress*, but too often both were missing but politicians often politicized intelligence. We saw over the last two years the opposing trends of high-tech intelligence, the obstacles of political hierarchies and decisionmaking on the tactical level, and the demands of hybrid and asymmetrical warfare. Intelligence operatives who talked recently to the author in Washington, DC and Brussels called intelligence and current procedures as *dysfunctional*.

Intelligence looked for better answers and U.S. tactical commanders began to bypass organizational obstacles and used artillery, tactical aircraft and especially UAVs to attack Taliban forces within Afghanistan and Pakistan whenever identified. The Taliban have adopted a warfare without communication means, learned to use the civilian population as shields, simply implemented Mao's idea of blending with the civilian population and take advantage of "enforced" support and some local sympathy, therefore undermining quite effectively the weak central government as puppets of "western occupation forces".

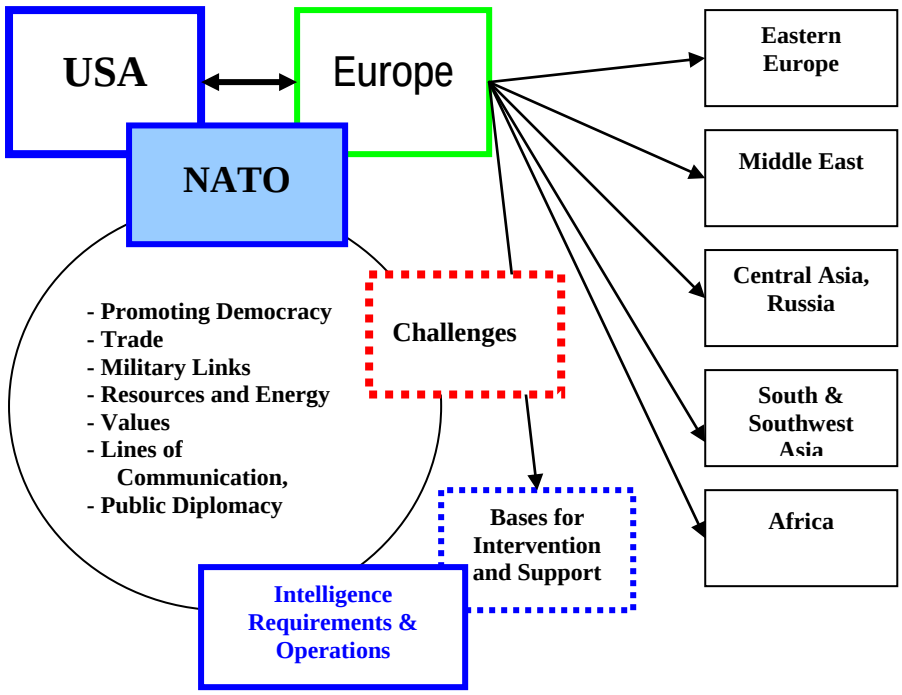
Field commanders complain about too long and complex procedures when asking for aerial reconnaissance and report of delays (up to three days!) before obtaining requested intelligence data, which became useless after such hierarchical delays. The new FM 3-24 *Counterinsurgency* has partially undermined efforts to kill as many insurgents as possible because of fear of civilian casualties and collateral damage.

Afghanistan is a war fought under similar procedures like Vietnam: In Vietnam it was airpower which was contained by the White House, in Afghanistan it is the new counterinsurgency "strategy", which limits military efforts. Like in Saigon, there is a corrupt and incapable government in Kabul that undermines politically and strategically what might be won militarily and tactically. The problem is political: Strikes against Taliban forces which kills too man civilians will erode the central government, but not killing Talibans would also erode the weak, insecure and unpopular central government.

There is even a larger political picture: In the eyes of Pakistan, a “democratic” pro-western Afghanistan is a possible ally of India, and Indian intelligence is working inside of Pakistan to use some clans to undermine the current Pakistan government. The Pakistan army needs the Taliban as an ally against India. When the Pakistan government turned to the west and ousted a number of high ranking military officers, the Taliban had suddenly lost support (and logistics) and looked for India and China as new allies. But China is not supporting Islamist radicals, neither does India, but there is Iran, which offered support. But there are Chinese and Pakistani interests involved, and the Taliban are more and more split up into factions used by all involved parties against other parties and with changing allies and priorities. This has helped the Pakistan government to contain the Taliban and undo former “safe havens” in western and southern Pakistan, which were until recently under the control of the Taliban.

Also, one wonders, if the people of Afghanistan are really eager to be saved by NATO and U.S. forces.

Intelligence must look into all such issues, but evidently various European governments have different views about these developments, and this has an impact on NATO intelligence, which is formally blended into (a) a “formal” NATO view and (b) a number of very different national views, which do not match.



NATO and Europe are bridges for the access to the Eurasian and African resources and trouble spots.

There are hundreds of books and thousands of articles written on intelligence: The CIA, the FBI, German, British, French or Soviet/Russian intelligence, their operations, directors, real or assumed mistakes, all became subject of numerous books and thousands of articles. On the other hand, there are only a few books written about NATO, mainly about its early beginnings, or of NATO in relation to national security and defense policies, also there is the *Handbook* (the current one is outdated).

But there is no book written about NATO intelligence. Even official NATO publications, like *NATO Today* (always written in the style of documents) rarely mention intelligence. Intelligence is only shortly mentioned in key NATO documents, and there are some *Allied Joint Publications* (AJP-series) and *Standardization Agreements* (STANAG). [1]

Many people believe that the alliance has a strong and very active intelligence agency on hand, but in fact there is none. And there are also people, who do not even know that NATO has a very active intelligence branch.

NATO intelligence, in the way it exists today, is the result of the early years of NATO, when it was assumed that all NATO forces would remain under national command, and strategic intelligence would be mainly national intelligence. Each nation would separately and "statistically" collect data on Warsaw Pact nations and their forces. This deficiency was partially repaired, when it became necessary to maintain a closer observation of the Warsaw Pact forces in the 1980s, but NATO`s intelligence branch always obtained the mass of data from U.S. agencies (mainly the DIA and military G-2/A-2 branches), and from some other governments like Great Britain, Norway, Turkey or Germany.

All other data, like battlefield intelligence (tactical level intelligence) and intelligence sharing, would - like the western allies practiced in the Second World War - begin when the shooting starts.[2] In fact, NATO intelligence always was a combination of Alliance and national intelligence.

In 1990/91, NATO intelligence was mainly canceling out week-by-week Warsaw Pact and Soviet force figures, and stopped rewriting threat estimates. When it was clear that the Warsaw Pact was a thing of the past, many governments in Europe had the opinion that intelligence was a Cold War relict. At the same time, the west and NATO faced an ongoing aggressive and large-scale Russian espionage agitation, but the political level largely ignored such.

The warning of experts (like the author) and historians about Russian behavior and a "remember the past, Russia did always come back"-type of conclusion outside "the End of History" loop, was seen as a contradiction to the new utopian political idealism of a new age that would end all wars with a new peaceful Russia, which - so the predictions - would become a kind of western democracy.

The idealists were wrong – as usual.

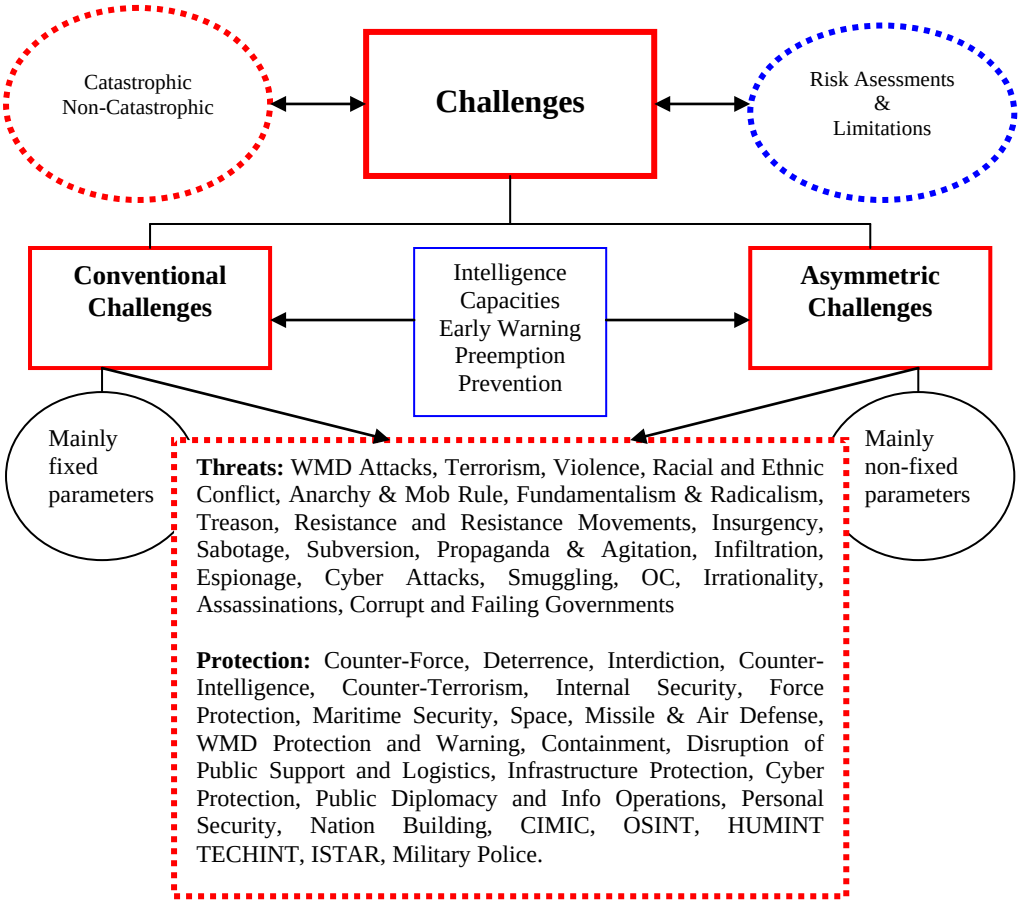
Within NATO, political guidance and allied planning for intelligence will come from the *International Staff*, the *Military Committee* and the *International Military Staff*, but active intelligence always remained in the responsibility of SHAPE and its G2 (now J2) division. But G2 was only a "receiving" staff section to collect force figures and technical or tactical data of Soviet and Warsaw Pact forces.

During the Cold War, for the defense of Western Europe, NATO nations were given large Corps Sectors, running from Denmark to the Swiss border, only air defense was centralized, and air assets were more integrated. National intelligence was mainly looking into such sectors.

Only SHAPE and some high staffs of NATO are truly *joint*. NATO forces are in peacetime rarely *combined*, but there were instances when NATO member- and PfP member-troops were *combined* in battalion-size organizations like in the Kosovo in 1999 and after.

Like in Germany before 1990, also in Kosovo nations were responsible for their assigned sectors, here for brigades and battalions (some multinationally structured), but such sectors became quite large in Afghanistan after 2003. The purpose is to create clear and visible zones of responsibility. That such separation can cause problems was seen in the Balkans[3] and is

seen again in Afghanistan. But all forces, no matter if operating under a NATO or a U.S. force commander, or a joint staff, remain largely under political control of the nations who contribute to such missions. The reasons for this are different national laws, caveats to the standard NATO *Rules of Engagement* (ROE), operational and tactical procedures, logistics and replacements.



Intelligence must prepare for a large array of threats and counter measures, which might require many years and high investments in resources and manpower.

What quality does intelligence within NATO have? One has to, as already mentioned before, distinguish between NATO-level knowledge and national-level knowledge:

- During the Cold War NATO intelligence was basically political and military intelligence plus some economic analysis of the Warsaw Pact member states; the overall knowledge was quite good. Because of its strategic nature, intelligence provided by NATO, required national intelligence gathering when looking for "details".
- Knowledge-levels of member-state intelligence were quite different, and this became evident especially during the Yugoslavia break-up; some states had excellent insights about the ongoing events, some had none at all. Intelligence sharing on the tactical level was always a problem.
- Afghanistan was until 2001 neither of any interest within the Alliance intelligence gatherings, nor of national intelligence of member-states. All intelligence was built up

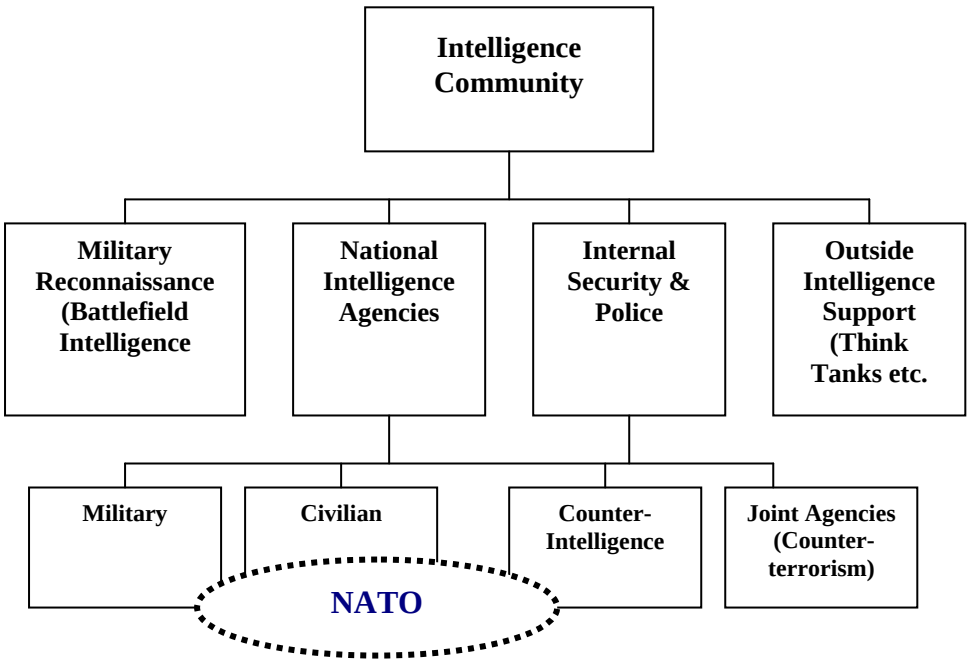
over a number of years but is currently still mainly political and militarily. But this will change into “cultural intelligence”.[4]

- Internet, TV-News channels and excellent newspapers provides strategic intelligence for all: Such Open Source intelligence is timely and is available for everyone; political levels do not have much different or more detailed information, and intelligence agencies usually have to monitor the news to be up-to-date.

Organizationally, NATO-level intelligence was and still is embedded in the joint staff structure and serves the political and military staff, but also supports lower levels of national defense staff requirements. Operationally, national intelligence serves on the strategic level as a gap-filler and is the main actor on the tactical level like in Afghanistan. Certain information is also distributed to some NATO *Partnership of Peace* states, and will be provided by such states to NATO as well.[5]

Using political science jargon, NATO is a *collective defense* organization, but serves also *cooperative defense* needs like the UN.

NATO slowly began to expand its data collection into new areas like North Africa, the Balkans, the Middle East, Central Asia, the Russian Federation, Afghanistan, Iraq, and involves counterterrorism, counterinsurgency, and counterintelligence. Intelligence organizations are civilian and military ones, often they are mixed.



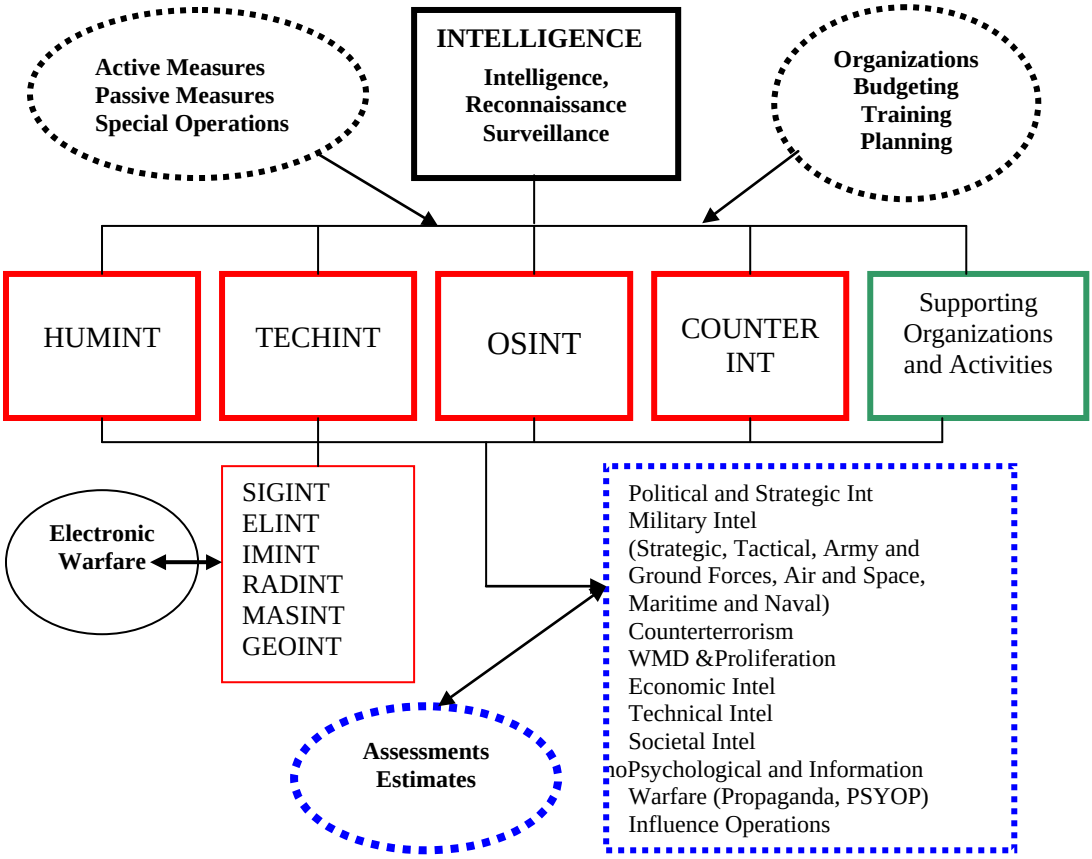
Challenges are not pure military one (in fact they really never were) but include a large array of possible threats. This expands intelligence in new areas and involved NATO intelligence in the Kosovo and in Afghanistan collecting political information on village level and clan levels, had to look into the local crime scene, reconstruction tasks, democracy building, drug dealing and local attitudes of people.

However, some of the old problems are hard to overcome, also in Afghanistan: The J2 ISAF MajGen Michael Flynn, went public on January 5, 2010, when he complained the lack of actionable intelligence provided by the troops and to the troops. Information from other sources (including NSA, CIA) is of low quality, “spies” were running around “killing

insurgents", but did not what they were supposed to do, and are out of touch with the Afghan people.

Intelligence activities require more and more people and especially people with knowledge in foreign languages and especially in languages, which were considered as "exotic" years ago and are now in high demand.[6]

Intelligence is also "learning by doing" and intelligence follows lessons learned and certain well-established procedures. There is a need to maintain a sound basis of knowledge to understand further developments and to expand from there into new areas. Intelligence needs the historian as a valuable expert to explain the past and to understand current events.



Overview of the mainstreams of Intelligence

Another urgent question is the quality of intelligence people. The failure to identify a Nigerian terrorist with the name Umar Farouk Abdulmutallab, despite a number of warnings, and have him boarding a Delta airline flight on Christmas Day 2009 to Detroit and the fact that he could do this only with the support of at least one individual on the Amsterdam Airport, NL, must be seen not so much as an organizational problem within the U.S. intelligence and counterterrorism structure, but as one of the people hired for the job which is to identify threats. However, as we have seen in the past, even experts can be wrong.[7] This incident pushed the proposal for a *National Threat Identification and Priorization Assessment* (NTIPA) to cross check all information by all agencies.

Farouk had the advantage that his name was spelled wrongly into the computer in the US Embassy in Abuja when his father warned the embassy. On November 20 his name was sent with a *Viper* message to the *National Counterterrorism Center* (NCTC). The CIA corrected

the faulty name spelling in the message and fed it into the *Terrorist Identities Datamark Environment* (TIDE) File, which contains 440.000 names, but he was assumed to be in Yemen. The FBI checked Umar via its *Terrorist Screening Center*, but in Nigeria the wrongly spelled name remained unsuspicious and Umar had since 2008 a two-year visa for the USA and in the State Department this name was not connected to the suspect. The next error was that the corrected name was not sent by the NCTC to the State Department. There were 4400 persons with a valid visa blocked from entering the US but not Umar. This case was the reason for changing the *Foreign Affairs Manual.*

John Brennan, Assistant to the President for Counterterrorism and Homeland Security, said on Jan. 9, 2010, that the people doing this job "didn't understand intelligence". So we have an intellectual problem, which affects the *National Counter-Terrorism Center*. One can blame it on the "non-discriminate"-type of hiring of definitely unqualified or unfit persons, but such is a too important job to be given to people with a few semesters of college education somewhere in Maryland or Virginia.

The Christmas 2009 incident was the reason for a number of further steps: New is the *Intelligence Executive Committee* (EXCOM) chaired by the DNI; new are *Rapid Analytical Support and Expeditionary Response Teams*, who will support the Pentagon and commands during preparations for interventions and contingency planning.

Many observers pointed to a number of intelligence failures and proposed new reorganizations, but organizational changes will not have much impact on shortcomings which are mainly based on personal or intelligence culture and working styles.[8] The proposal to eliminate the Director of National Intelligence (DNI) is not a new one.

Dennis C. Blair, the Director of National Intelligence, wrote in the new version of the *Information Sharing Strategy of the United States Intelligence Community*, the intelligence organizations must adapt to the new threats:

„*We must be agile: An enterprise with adaptive, diverse, continually learning, and mission driven intelligence workforce that embraces innovation and takes initiative.*"

Threats are coming from China, Russia, Iran and North Korea, come from insurgents extremists, terrorists and transnational criminal organizations. The economic circumstances will additionally feed such dangers and will raise the number of „ungoverned spaces", of failing and failed states. The proliferation of weapons of mass destruction is continuing, new threats are *cyberwarfare*, which underlines the needs of *cybersecurity* and *cyberintelligence*.

Cooperation with allies is a must and politics must support the tasks of the „Intelligence Community" (IC). Main tasks are strategic early warning, counterintelligence, and the support of the armed forces. Blair was continuing, what in February 2008 the former DCI James M. McConnell and the Associate Director of National Intelligence and Chief Information Officer/Intelligence Community Information Sharing Executive, Dale Meyerrose had written in the former *Information Sharing Strategy of the United States Intelligence Community.* The IC must change their habits of not sharing intelligence. The new tasks are „Responsibility to Provide", „Mission Centric", „Information Centric", „Across Agency Service" and "multidimensional analyses". The IC must invite experts from many areas like politics, society, technologies, economy, culture etc. The new approach will replace the former „Need to Know" and „Agency Centric"-orientation of the IC. MITRE in McLean, VA, recommended information sharing on a multinational scale to support the allied forces in Iraq, Afghanistan, and South Korea, but also the fight against terrorism.

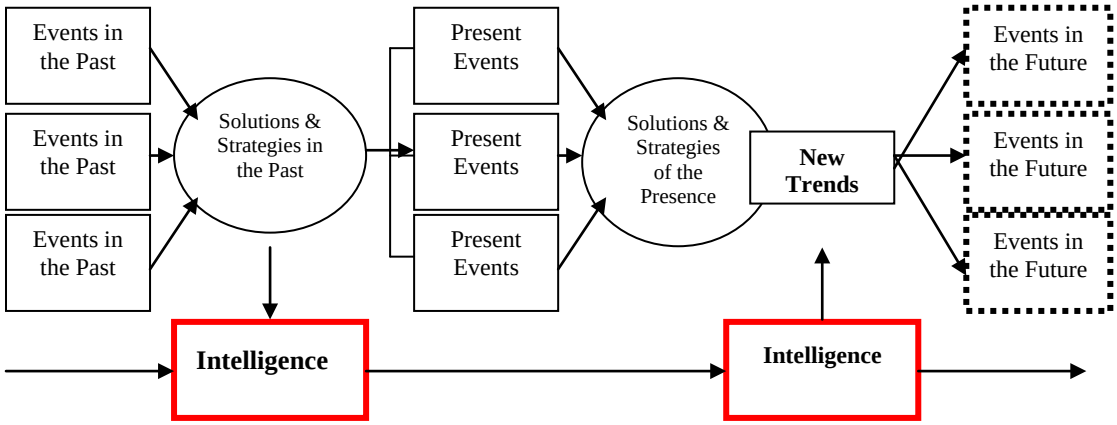
Within NATO a number of committees are dealing with information warfare, like the NATO *Consultation, Command and Control Agency*. New is also the invitation of experts for NATO`s *New Strategic Concept.*

President Obama and Dennis Blair want retired intelligence officers and CIA experts and veterans back as advisors and teachers. The selection of John O. Brennan as White House top adviser on terrorism was a first step in this direction. This also includes a number of think tanks and experts in corporations. Fusion centers are another step, including FBI, CIA, Homeland security and the Defense Department. Leon E. Panetta, Director of the CIA wants to transform the agency into highly respected organization of the "best and the brightest" and is hiring the best students in universities.[9]

Finally, the President pushed a *National Cyber Strategy*, which should be ready in the summer of 2010 and will be a framework for a possible NATO document in 2011.

The new FM 2-0 *Intelligence*, released March 2010, underlines the importance of intelligence for planning, threat characteristics, operations, force generation, situational awareness, demands ISR integration and continuous input.[10] Operational and tactical intelligence was delineated in e FM 2-01.2/MCRP 2-3A *Intelligence Preparation of the Battlefield/Battlespace*.[11]

The *New Strategic Concept* for NATO, currently in the final editing, will, if compared to the NATO *Strategic Concept* of 1999, include a dozen of new topics.



There is a learning process in intelligence, which spans decades and generations of experts

The aim of this study is to look into the recent achievements and improvements accomplished over the last years, and to give some ideas how NATO intelligence works. It is information about the tasks of intelligence in the Alliance, the state of the art, ongoing problems, and about certain improvements.

In the meantime the U.S. Intelligence Community created an *Intelligence Community Information Sharing Executive*,[12] and published the *Information Sharing Strategy*,[13] and a new *National Intelligence Strategy of the United States of America*.[14] Information Sharing Strategies were also released by the Department of Defense, the Department of Homeland Security and the FBI.

The reader will understand that the author will, for security reason, withhold certain sensitive issues regarding NATO intelligence. Because of a number of functions, he is also accountable to security regulations of the Austria Ministry of Defense.

NATO Gets Better Intelligence

New Challenges to Intelligence

There are traditionally three levels of intelligence (even when such separation was always quite artificial), however there is now a fourth level, which has an impact on intelligence operations and assessments:

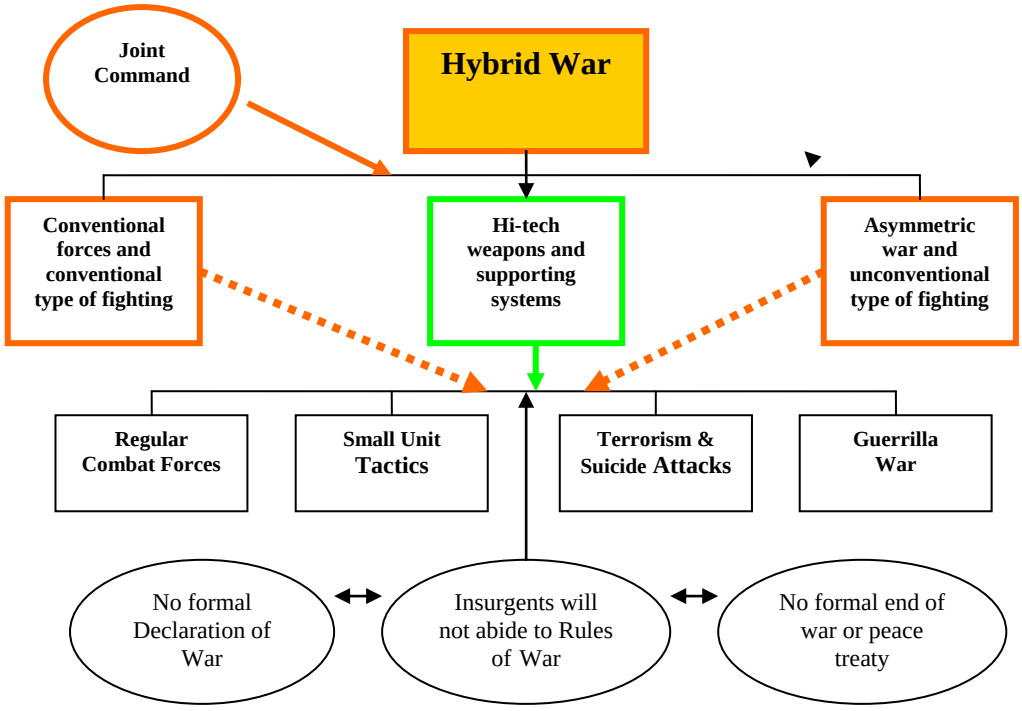
- ***Strategic intelligence*** is basically political intelligence and large-scale forecasting on possible antagonist or hostile governments, and is usually delineating and generalizing current and expected political developments; the military strategy level includes weapons of mass destruction (WMD), force postures and their capabilities and other powers, and their probable involvement in a given crisis or conflict.[15] Strategic intelligence is the fundament for the Phase I of an intervention/war planning process.
- ***Operational intelligence*** is "current intelligence", tailored to the need of deployed (blue) forces, it includes all aspects of red forces, like leadership, force organization, dislocations, readiness, mobilization, foreign suppliers and possible technical capabilities, and is needed for an operational estimate on enemy forces and other data needed in Phase II planning and force deployments; it is geographically covering the whole operation area, will include political, social and cultural aspects, and is usually prepared by military and civilian experts. Current operations and operational intelligence will also include adjustments of military commands, new types of combat forces (Brigade Combat Teams, BCT), supported by *Asymmetric Warfare Groups* (AWG, assessing special combat area requirements), a *Rapid Equipping Force* (REF, providing specific combat zone needs for a deployed BCT), [16] and the Air Force created in 2008/09 *Contingency Response Wings*.
- ***Tactical intelligence*** is "present actual intelligence", needed and produced by employed troops during Phase III (tactical operations) in various types of war, especially hybrid war. It is a combination of operational information plus tactical combat data and developments, including data on guerrilla forces, counterinsurgency requirements, local civilian attitudes, terrorism and gang warfare, but also looks out for new threats, gaps in blue force defense, and red force tactical misjudgments, local political and ethnic developments, and nation building problems. Additionally, tactical intelligence gets now NATO`s *Consultation, Command and Control Agency* (NC3A) support, like communication, specific intelligence networks and situation awareness; intelligence is furthermore supported by a *Multisensor Aerospace-Ground Interoperable ISR Coalition* (MAJIIC) Network.[17]
- ***Comprehensive Intelligence:*** It includes hybrid warfare specifics, and Phase IV operations (pacification, occupation, nation building/civilian support, withdrawal of blue forces). It requires a comprehensive approach, supporting *Civil-Military Country Teams* and C*ooperation* (CIMIC), *Civil-Military Reconstruction Teams*, and small squad-size *Human Terrain Teams* to contact local authorities, plus the cooperation with NGOs. U.S. Field Manual 3.24 *Counterinsurgency* (2006) reminds policymakers that planning for nation building must be included already during strategic and operational planning (Phases I and II) - therefore in advance of any intervention. Nation building/societal building must begin when combat operations (Phase III) are winding down.[18] *Cultural Intelligence* is now included in manuals about all kind of operations like stability operations, peace support operations, and tactics (see FM 3.0 *Operations* and FM 3.24 *Counterinsurgency* etc.).[19] Postponing "winning hearts and

minds"-work until Phase IV is seen now as an invitation to disaster and might extend *short war* scenarios to *long wars*.

In each intelligence category, timely and accurate intelligence is the foundation of success. When the shooting starts, tactical and HUMINT intelligence is more important than strategic intelligence. TECHINT, (like SIGINT) is mainly supporting, surveillance and ongoing reconnaissance brings additional situational information. The tracking of friendly forces is also of importance because it helps to avoid confusion and friendly fire. The issue is never either HUMINT or TECHINT, but always a combination of both.[20]

Hybrid Wars

Interventions of U.S. and NATO forces in Somalia, Afghanistan and Iraq were facing a war, which is a hybrid of different kinds of threats, characterized by an absence of *ius in bello* or *ius ad bellum* (the rules of the Hague Agreements or of any Geneva Conventions), sees neither peace nor war, is a mix of regular/conventional and irregular war with mainly asymmetric attacks plus civil war. Pacified regions can exist next to war zones, but can become war zones again or see terrorist attacks.

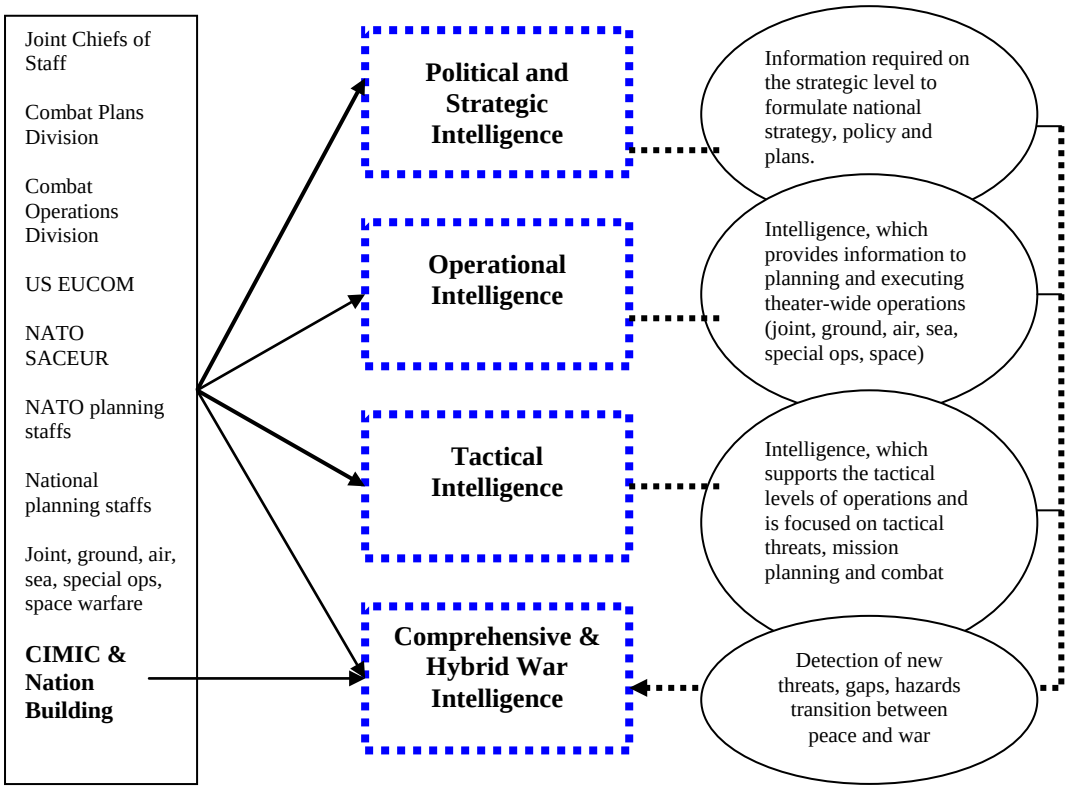


The new threats intervention-forces are facing are a mix of conventional and asymmetric fighting enemies where regular forces mix with irregular forces and terrorists.

Hybrid war is war without borders; there is no declaration of war, no formal ending of war, and no peace treaty. There is no separation of soldieries, civilians, terrorists, insurgents, religious fanatics and criminal killers. Hybrid war will include terrorism and cyber war, and can last for a decade and more. Is traditional warfare centred on the enemy's government and military, irregular war or hybrid war is aimed foremost on the population (which must be considered by both sides at least as partially hostile). A government and its forces supported by blue alliance forces will usually be targeted. Irregular warfare is also without a clear *Center of Gravity*.

Hybrid war has a dramatic impact on intelligence. Counterinsurgency operations and tactics are the main tool in fighting such wars. It is based on good tactical/comprehensive intelligence, and requires constant communication with the population.

The U.S. government and the new CENTCOM military leadership (Generals David Petraeus, Stanley McChrystal, Raymond Odierno) and new strategy papers and field manuals like Joint Publication 3-05.1,[21] FM 3-24, [22] or AFDD 2-3,[23] are reminders that knowledge and experiences won in limited and counterinsurgency wars (COIN), all well established in World War II and Vietnam, were all forgotten.



The current relationship of Political-Strategic, Operational, Tactical and Comprehensive Intelligence within NATO

Long War – Short War

One typical error of all war planners since 1900 is the assumption that always the next war would be short; after victory, life would go on undisturbed and troops would go home. In fact, most wars are long, like Korea, Vietnam or now Iraq (finally winding down) or Afghanistan. The Gulf War of 1991 was very short, pre-decided by airpower, so was the air war against Serbia in 1999. Iraq in 2003 was in Phase III a short war, but it did not end as anticipated. The war in Iraq lasts now for more than six years, even when now winding down it still has the potency to escalate again. The civil war in Somalia had no clear beginning and sees no end either.

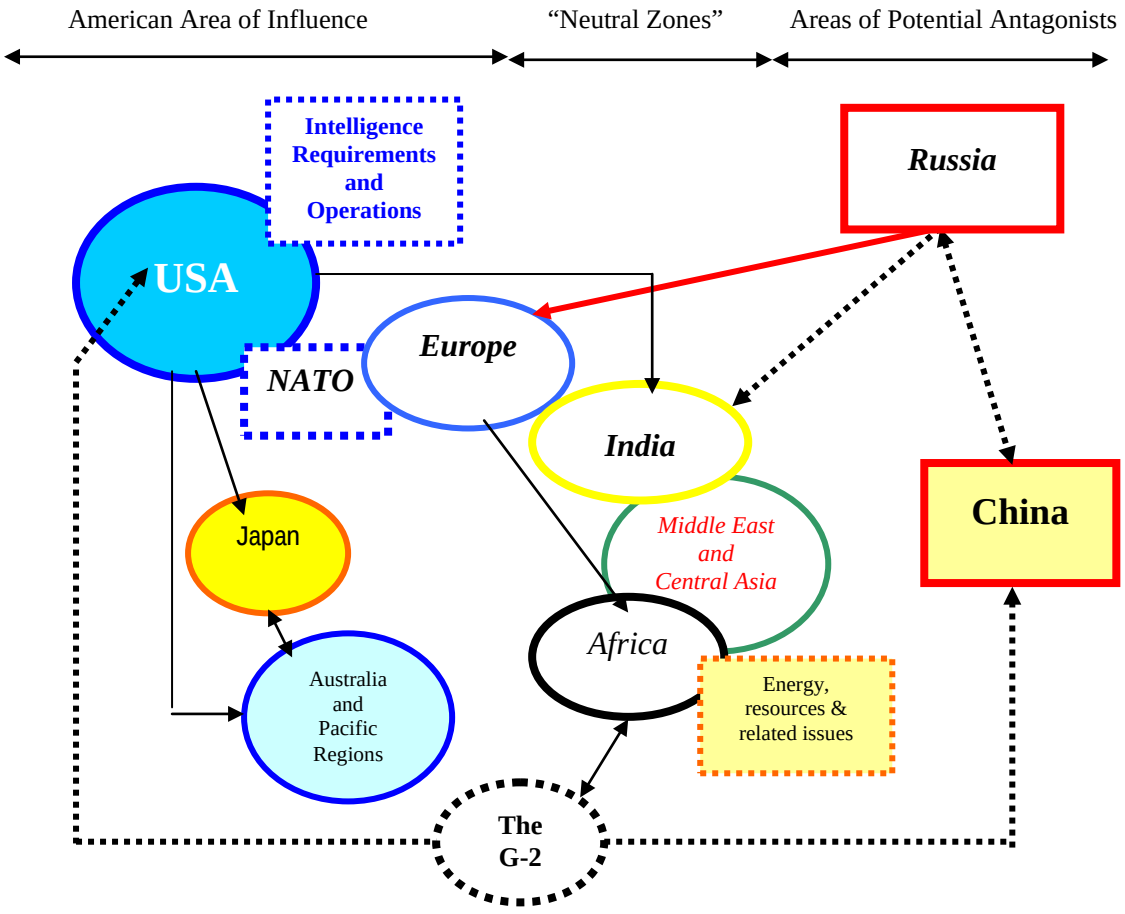
U.S. Intelligence – Guidance for NATO

Earlier Intelligence Reorganizations

NATO is dominated by the United States, and NATO intelligence is dominated by U.S. intelligence intentions and procedures.

The United States in the years after the *National Security Act* of 1947 saw always a need for military reform, but besides the creation of the CIA, NSA and DIA many decades ago, changed the military and civilian intelligence organizations only sporadically.[24] Even when the powerful *National Security Council* was reorganized by each President, the intelligence structure below was rarely altered, and if, mainly administrative issues. Many commissions and boards (so under Eaton, Schlesinger, Taylor, Childs, Murphy, Church, Pike, Simon and others) recommended minor or larger changes, but they were mainly ignored.

The *National Security Agency* (NSA) was created in 1952, the *Defense Intelligence Agency* (DIA) in 1961. Small changes did occur during the presidency of Eisenhower, Nixon and Ford. Of consequence were E.O. 11905 and E.O. 12036, but many changes came with E.O. 12333 of December 4, 1981, signed by President Reagan, which extended the scope of intelligence and operations.



US intelligence requirements involve the whole world

Congress (*Senate Select Committee on Intelligence, House Permanent Select Committee on Intelligence*) often demanded not only budgetary oversight, but also supervision of activities

and even of secret operations as written into the *Hughes Ryan Act* of December 1974, and proposed by the *Church Committee* report in 1975. Congress also debated for decades about improvements in intelligence, voted for the *Intelligence Oversight Act* of 1980, which demanded prior information of Congress about major clandestine operations, followed by the *Intelligence Oversight Act* of 1991.

These must be seen as fallouts from the Watergate affair, but intelligence knew how to overcome such demands and rules: The White House and the intelligence organizations insisted on their right to keep "top secret" documents locked, and sensitive activities out of reach of any Congressional oversight. The large number of organizations and reorganizations, and hundreds of ongoing operations, made supervision anyway impossible.

Recent Intelligence Reorganizations

30 different organizations today have a budget of 75 Bio. US $,[25] and employ some 290.000 people.[26] Many of these reforms had an impact on NATO.

Non-Military Intelligence Reforms

President Clinton looked into a more innovative intelligence structure in 1996,[27] but the agencies were slow in changing their habits. However, the "9/11" attacks initiated a number of reorganizations, some based on the *Patriot Act* of 2001,[28] some on Executive Orders signed by the President. [29]

In 2002, the joint *National Commission on Terrorist Attacks Upon the United States* recommended a far-reaching intelligence reform, which resulted in the *Intelligence Reform and Terrorism Act* (IRTA) of 2004, who saw the creation of the *Director of National Intelligence* (DNI) and of a *National Counter-Terrorism Center* (NCTC, (400 employees) located next to the CIA compound. Other laws were amended, like the *Foreign Intelligence Surveillance Act* of 1978.[30] The *Secret Service* and Coast Guard Intelligence were moved to the new *Department of Homeland Security*, a move that was not really understood. The *National Intelligence Agency* (NIA) is the successor of the *National Intelligence Council* (NIC)[31] and was shifted from the CIA to the DNI: It is a rather small instrument of the Director of National Intelligence (DNI), and will finalize estimates which in fact are basically CIA estimates.[32]

President Bush also installed with PDD 75 a *National Counterintelligence Executive* (NCIX).[33] In 2005 and in 2008, more changes came along with additional revisions of E.O. 12333, which altered again some of the revisions made in 2004.[34] However, changes in the organization alone were not being the only answer to improve conditions.[35] "9/11" was not only an intelligence failure, but also one of established airport and airline security policies and procedures. However, organizational changes like the ones of 2003/2004 could not overcome all inadequacies,[36] therefore, new approaches were needed, and especially the *Collins-Lieberman Bill* (July 2004) had a tremendous impact on Congress and the intelligence community. In summer of 2009, the CIA Director Leon Panetta was in a fight against Congress and accusations against the CIA.[37] Panetta in public statements had attacked House Majority Leader Nancy Pelosi. Other issues were the different opinions on intelligence priorities between the DNI, the Director of CIA and the, the Director of the FBI, with James Jones as National Security Adviser in the role of mediator.[38] The CIA won over DNI Denis Blair, when Blair insisted to have its own personnel stationed in U.S. embassies.

Only the intelligence and security branches of the State Department (*Bureau of Intelligence and Research, USIA, AID, Embassy Security* and the *Bureau of Diplomatic Security*) remained unchanged and also remained fully "civilian".

Military Intelligence Reforms

In 2002, the U.S. Department of Defense implemented new directives for the military agencies, which had an impact on organizations, hierarchies and reporting. The military also protected its intelligence services and their roles, and even inside the armed forces the intelligence branch expanded and remained untouched by Congress.[39]

A number of intelligence reforms were implemented. The Department of Defense saw the creation of the *Director of Defense Intelligence*, a position that was combined in May 2007 with the *Under Secretary of Defense for Intelligence*, created in 2004 by the IRTA.[40] For the first time, all Department of Defense intelligence agencies (DIA, NSA, DSS, National Geospatial Intelligence Agency, National Reconnaissance Office, the intelligence organizations of Army, Navy, Air Force, Marine Corps and the attached intelligence branch of the US Coast Guard), came under one supervisory authority, which is basically a budget-oversight.

Quite interesting is the fact, that generals and admirals gained control of all major civilian agencies with exemption of the FBI. LtGen James R. Clapper, the former Director of the National Geospatial Intelligence Agency, and of the DIA, became the powerful Undersecretary of Defense for Intelligence. The current Secretary of Defense Robert Gates spent 27 years in intelligence and was Director of the CIA from 1986 to 1989.

U.S. military intelligence certainly outreached over the last years, and one has to add the tight cooperation between U.S. and British intelligence, the British-French cooperation, and the German and Italian services with their detailed knowledge of various regions in Europe, Asia and Africa. Australian intelligence with their listening posts directed to Southeastern Asia, is an important source for U.S. and British agencies, and therefore also for NATO, so are Japanese and South Korean findings. France is one of the best sources of sensitive data regarding a number of “hot areas” in Africa and the Middle East.

Further Changes

Many authors complain that the last round of reorganizations had not resulted in any measurable improvement.[41] Admiral Eric Olson, commander Special Operations Command (SOCOM), was recently discussing the war in Afghanistan in Washington, DC, (NDU/NESA Center) and reminded the audience that industry is developing numerous systems to find, analyse, track, and communicate information, but the troops must be adequately trained to use this equipment and combine sensors, computers and personnel. Here he sees room for improvement. Others see the future in a homogenized combination of OSINT, HUMINT and UAVs.[42]

Another issue is cyberspace security and the creation of the U.S. Cyber Command (USCYBERCOM), as an additional unified command of the Defense Department.[43] A *United States Strategic Cyberspace Strategy* will be published in 2010.[44] Relevant intelligence regulations include JP 2 series, FM 2 series, AFDD 2 series, OPNAV manuals etc.

Presidential Findings

Ordering clandestine operations requires a Presidential overview and consent. According to Section 622 of the *Foreign Assistance Act* of 1961, the President must approve or order intelligence covert actions (“special activities”, see also Section 501, *National Security Act* of 1947) by a written *Presidential Findings* (PF) document, which is based on a *Memorandum of Notification* (MON), usually written by the CIA or the DNI.[45]

Such binds the CIA or any other intelligence organization; if such an activity has to be altered or cancelled, the President must approve any such change as well. It is understood that routine operations are not subject of any forwarded *Notification* and *Findings*.[46]

Intelligence and the NSC

Since 1947, the NSC is the main arbitrator for intelligence activities and is more or less also the final authority. Many changes have altered responsibilities and supervision. Various NSC committees and planning groups often changed their names and structures, but involved always the President, Vice President, National Security Adviser, Secretary of State, Secretary of Defense, Director of the CIA, (and since 2004) the DNI, the Chief of Staff to the President, the Chairman of the Joint Chiefs of Staff, and the Counsellor to the President. Others, like experts, the Director of the OMB, the Attorney General, or the Director of the FBI might attend.

The Links Between U.S. Defense Requirements and NATO

NATO is basically providing the important link between U.S. and European security requirements in the Northern Atlantic-EUCOM region. From a U.S. geopolitical-geostrategic point of view, it permits the U.S. to control of the "opposite coast", which is seen by strategy experts as a paramount U.S. security requirement. NATO is fulfilling this task, and the U.S. is paying back with security guarantees.

Seen from a geopolitical point of view, the United States wanted after 1945 to contain any power or any combination of powers on the Eurasian landmass, which might become a dangerous challenge for the security of the United States.

The improving relationship between NATO and the European Union will have an impact on the sharing of intelligence as well.[47] Russia is emerging again as antagonist to the west and to NATO; this fundamental and geopolitical change will have a decisive impact on national intelligence and NATO intelligence and new strategy papers.

For Europe, NATO is a nearly perfect security umbrella against contemporary and future threats from the east, south, and southeast. This umbrella includes political cooperation, links to the European Union and other nations, which are cooperative partners, either within NATO or in other regions of the globe. These linkages include security agreements, nuclear weapons, conventional forces and also the sharing of intelligence.[48] As the U.S. has extended EUCOM and NATO to CENTCOM and AFRICOM, the same governments who send troops to Afghanistan were as EU-members insisting on a different agenda, based on *Soft Power*, international law and humanitarian considerations, with a public that strangely accepts NATO operations but declines military interventions by the EU.[49]

The Links to NORAD, NATO Air Defense, Missile Defense (Extended Air Defense) [50]

The U.S.-Canadian *North American Air Defense Command* (NORAD, Peterson AFB, CO) which operates the strategic Ballistic Missile Early Warning Systems of the United States, is linked to the NATO *Air Defense Ground Environment* (NADGE), a NATO owned air surveillance and fighter direction system, consisting of *Combined Air Operation Centers* (CAOC), *Air Operations Coordination Centers* (AOCC), *Sector Operation Centers* (SOC), *Control and Reporting Centers* (CRC) and AWACS aircraft.

NADGE is linked to national NATO air defense organizations (command centers, fighter bases, air defense missile sites, radar stations) and is currently transformed into the *Air Command and Control System* (ACCS) with relay-, data link-, satellite- and other communications. Great Britain operates its semi-national structured I-UKADGE system.[51] NADGE/ACCS consists of strategic level command centers, operational level CAOCs who prepare the Air Tasking Orders (ATOs) for combat units on the tactical level. The air picture provides real time data for the overall NADGE/ACCS structure, which is a valuable intelligence tool not only for the estimates of enemy air activities, but also for friendly (blue force) air operations, operational and tactical planning etc.

In the last years, ballistic missile defense became a major tasks and this includes extended air defense, early warning systems (radars, satellites), ground stations, communications, mobile air defense missile systems, like THAAD, MEADS and currently *Patriot* and other systems deployed in Europe.

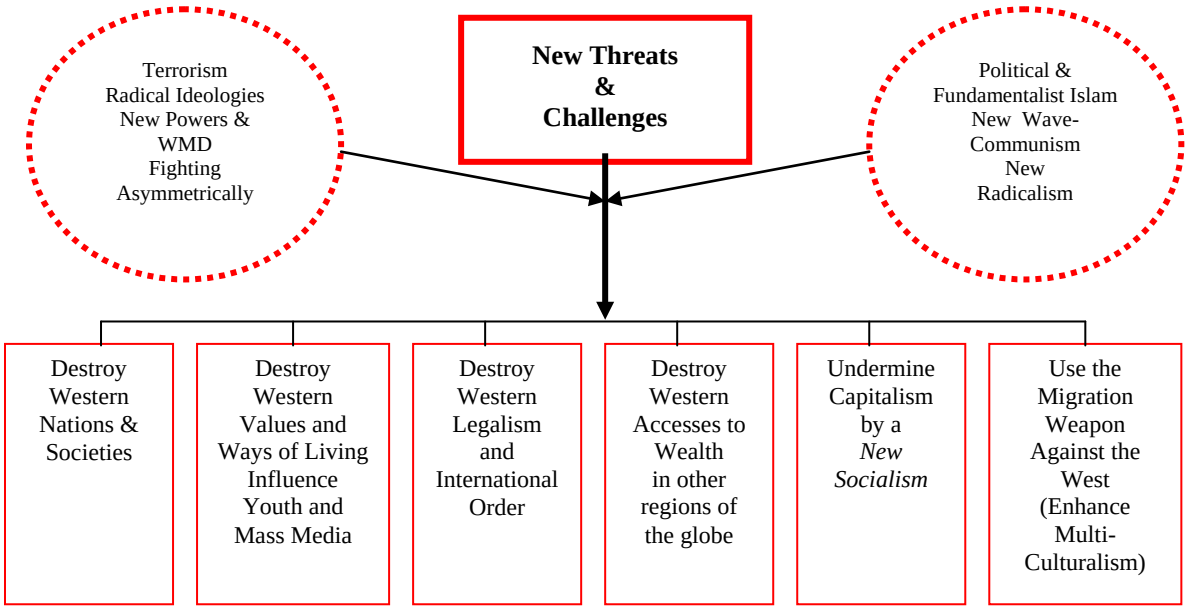
U.S.-NATO`s Intelligence Fusion Center [52]

The NATO *Intelligence Fusion Center*, RAF Molesworth, England, became operational in the fall of 2007 and employs 160 experts from many NATO members. It is basically a U.S. intelligence center for EUCOM and sits next to EUCOM`s *Joint Analysis Center* (JAC), but is also receiving data from close allies like Japan, Australia or South Africa. Certain information will also come from the *National Military Command Center* (Pentagon), the *Emergency Conference Room* (Pentagon) and the US *National Counterterrorism Center*. The *Fusion Center* provides around the clock (4 shifts) all-source strategic and tactical theater intelligence (ASAS), using also geospatial, air defense and targeting data.

It answers *Requests for Information* (RI) coming from all U.S. and NATO commands, will point to gaps in intelligence and recommends improved intelligence processing. It is structured into a command, an analysis, an operational and a support division.

The Center also supports the electronic battle plan, C4ISR/C4ISTAR, cyber defense and cyber attack planning and tactical and technological aspects. Intelligence is currently collected especially on the Middle East, on South Asia and Northern Africa.[53]

The authors of *Towards a Grand Strategy for an Uncertain World* recommended the transformation of this establishment into a Joint NATO/EU Intelligence Fusion Center.[54]



The threats and challenges of the 21st century, as seen by the U.S.

AWACS, J-STARS

The fleet of 17 E-3C aircraft of the Airborne Warning and Control System (AWACS) with 30 crews, and 6 additional Royal Air Force E-3Ds, are assets, which NATO permanently has for its own requirement and are providing a tactical air situation picture. AWACS are also airborne air defense command centers, directing friendly fighters to hostile platforms.

Additionally, France also contributes with its 4 E-3Fs. AWACS has a radar which surveys an airspace with a diameter of 250 to 400 kilometers or more than 200.000 square kilometers, depending on the flight level (normally 30.000 ft) and the radar cross-section (RCS) of a target. U.S. AWACS and J-STARS aircraft and NATO AWACS use JTIDS/Link 11, 22 and Link 16. New assets are the *Global Hawk/Eurohawk* UAV platforms, new satellites like the German SAR-*Lupe* or French *Helios* 2A/B, plus commercial sources like SPOT. J-STARS, based on Boeing 707 airframes have down-looking radars which provide data about static and moving targets up to a distance of 135 nm from the aircraft depending on the flying altitude. The air picture is sent to ground stations for real-time dissemination and fire support.

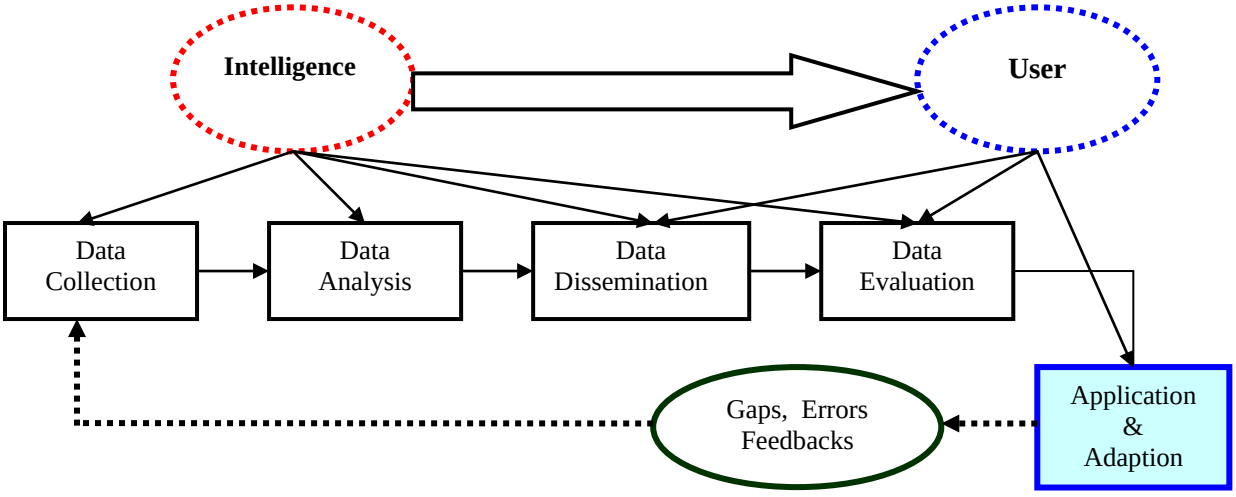
The USAF has improved ISR and trained 2500 men and women in ISR technology at Langley AFB,VA, filling a gap, which was identified in 2005. The Air Force will organize fusion teams, which are called Analytical Report Teams. The training requires six months

Civilian-Military Expert Teams

The U.S forces began in 1995 to add *National Intelligence Support Teams* (NIST) to their commands; they include experts from the CIA, DIA, NSA, NRO and J-2/G2/A2, based on the *Presidential Decision Directive* 35. They were followed by the *Rapid Analytical Support and Expeditionary Response Teams* (RASER-Teams), of civilian and military experts for the preparation and support of operations in crisis regions and counterterrorist activities.[55] The next step saw the creation of Civilian-Military Country Teams. The planning sees eight to ten such teams with strength of 1000 each for CENTCOM, AFRICOM and SOUTHCOM.

U.S.-NATO as Intervention Forces and New Intelligence Requirements

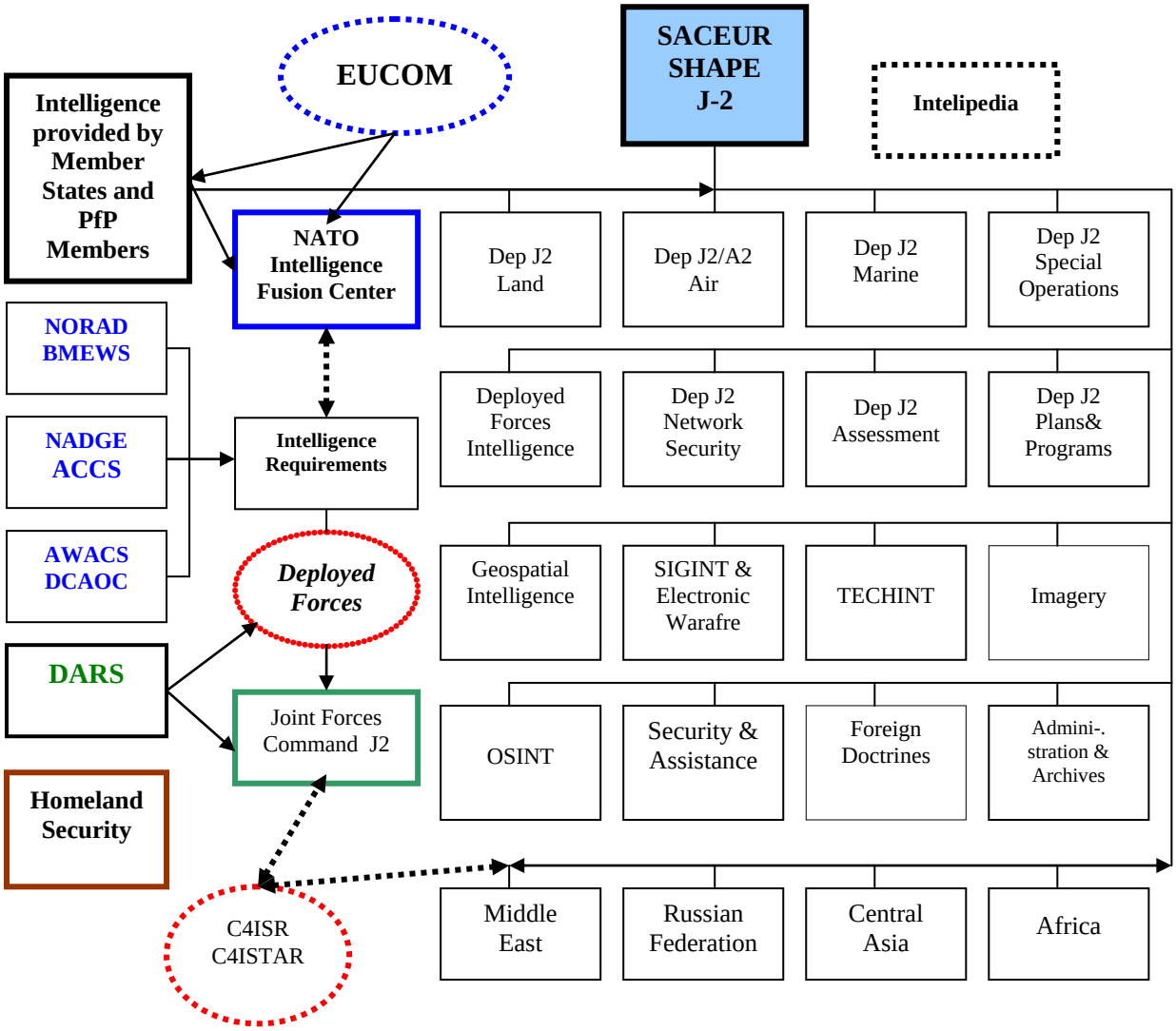
The current NATO-internal political disagreements and frictions were demonstrated by the resistance of European governments to deploy more forces to Afghanistan. NATO and EU have an identical anti-pirate-agenda for the western Indian Ocean, but the EU insisted on its own “soft” operations, which had problems to achieve its intended purpose. NATO and EU had to accept that national sensibilities, multinationality and force integration, national laws and an unwillingness to fight pirates effectively are certainly not supporting such missions but create obstacles.



From Data Collection to Application and the Feedback Process

No command in the field can work when each nation undermines operational command and control (C2) by numerous national exceptions and caveats written into the standardized

NATO *Rules of Engagements.*[56] Such will result in unworkable command relationships that are eroding military decision-making and execution. The meeting of former Secretaries of State (Kissinger, Baker, Christopher, Albright, Powell) at George Washington University on September 28, 2008, demonstrated bipartisan unanimity about America's willingness to intervene in Africa (Sudan, Congo, Somalia), but where are the European allies to form with America a *Coalition of the Willing*? Where is NATO?



The ultimate organizational structure of NATO intelligence includes all aspects. This graphic does not correctly resemble the current organization, which is subject of ongoing adjustments, but structures, which have been in place over the last twenty years.

In the Cold War, western intelligence was shaped to analyse the Soviet Union and the Warsaw Pact, including leadership, industry, the disposition of forces, readiness, training and logistics, technology, operational aims, tactics - all topics of paramount importance. Intelligence was quite good in analysing many details because the enemy was geographically and organizationally mainly "static". After 1990, the emphasis was shifted to economic analysis and terrorism. With the demise of the Soviet Union and the Communist block, military intelligence was widely seen as "improper", was "insulting" the new bonds between Europe and Russia. Even when Russia fell back in its former Soviet habits after 1998, the

European governments preferred to look the other way, also closer cooperation of western intelligence agencies was considered as “Cold War” activities.

Today, there are additional challenges for intelligence: Thousands of possible terrorists who act in global networks, the trade of chemical and binary-usable substances, the smuggling of explosives, of weapons, of parts to trigger bombs, money laundering and growing organized crime. There is large-scale hostile (Russian, Chinese) espionage, but containing such activities by counterintelligence and police, is not always appreciated by governments: Counter-intelligence should not disturb business opportunities and “good relations”.

Special Operations and CSAR [57]

Special Operations are embedded in the national forces of NATO member states and participating PfP-nations. NATO can use such forces if deployed to combat areas like in Afghanistan. Special Operations require first class intelligence to fulfil their mission but are also some of the best instruments to collect information.

Such activities also serve *Combat Search and Rescue* (CSAR) operations, which have the purpose to extract downed aircrews in hostile environments, geographically often deep behind enemy lines or forward edges of blue forces. CSAR depends fully on up-to-date intelligence, which includes the locating of pilots or crews, enemy activities and anti-aircraft weapon positions, weather, topography, fighter cover, back-up aircraft, flying-routes and altitudes, planning of air to ground fire etc. CSAR is also a tool to recover cut-off soldiers, and the insertion or retrieval of long-range reconnaissance teams (retraction).

ISTAR [58]

One of the most challenging long-term *Net-Centric Warfare* projects of NATO is the *Intelligence, Surveillance, Target Acquisition and Reconnaissance* program (ISTAR). ISTAR includes ground, air, space and naval means to find and identify hostile targets with high accuracy to transmit target data to blue commands and weapons on the “extended battlefield”. With the emergence of UAVs, such intelligence and surveillance can be extended to many hours and over large areas. Armed UAVs permit attacks in real-time. ISTAR was decided by the NATO Summit in Prague in 2002. NATO has invited the European Union to participate in these planning and EU is now participating, so is the European industry.

ISTAR will combine radar and other sensors, computers and radios, linked to a complex network. Originally funded by national budgets, and pushed especially by U.S. forces, NATO established in 2003 the NATO *Airborne Early Warning and Control Force* in Ramstein AB, Germany, as part of NATO Headquarters CC Air, and began ISTAR initiatives (as Forces Objectives) for the air, naval, ground forces for division and brigade-levels. ISTAR should also help to minimize collateral damage and support the identification of friendly forces. [59]

Cyber Security and Warfare

William Gibson coined the term Cyberspace in 1982, and John Perry Barlow used the term in connection with the Internet in 1990. The Joint Chiefs of Staff defined in their Joint Staff’s Joint Net-Centric Campaign Plan the cyberspace as:

A domain characterized by the use of electronics and the electromagnetic spectrum to store, modify, and exchange data via networking systems and associated physical infrastructure.

Additional explanations would include:

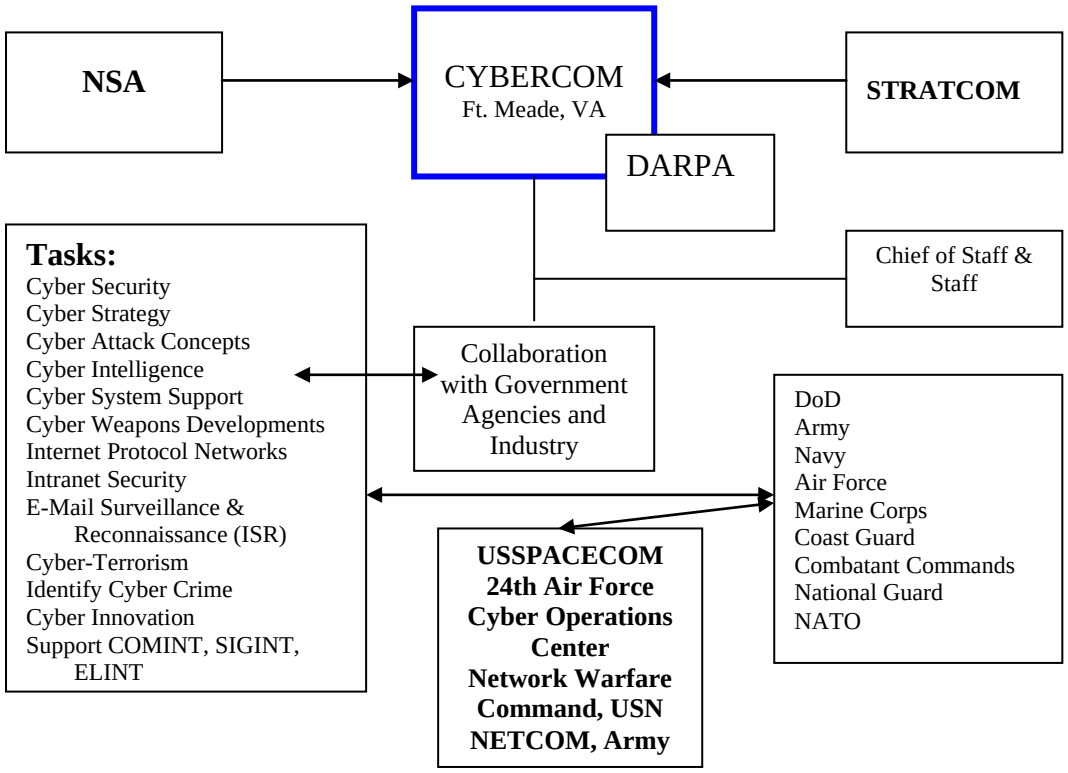
Cyberspace exists along the other warfighting domains and should be protected and exploited in a similar fashion. This reflects the need to gain and maintain operational freedom in cyberspace superiority – as a predicate to maintain land, air, and sea and space dominance.

In the last decade numerous government agencies in the US and NATO faced a growing number of cyber attacks. Cyber attacks are a part of electronic warfare and include electronic attacks against communication, computer and other systems, system-interruption, destruction, spying, illegal infiltrations and stealing of software and documents. The fact is that the Internet is very vulnerable and exposed to attacks. Cyber defenses are weak in inadequate; attackers remain mostly anonymous. US approaches to foreign government to arrest identified attackers were generally ignored,

NATO faces more that 100 cyber attacks a day, mainly from Russia and China, in the last year also from North Korea and Iran. Russia and China had infiltrated governments systems in more than 100 countries around the globe.[60] Russia attacked in 2007 the computer systems of Estonia and in 2008 the systems of Georgia days before the war began. China tries to prevent any foreign Internet information to the general public and tries to interrupt such networks on a permanent basis. Google was forced out of China in April 2010 by blocking out restricting more and more websites and uses such policies as part of its own information strategy and war against the west, South Korea, Taiwan, and Japan. 2009 and 2010 the attacks were aimed against computer systems of many non-government institutions like the New York Stock Exchange, NASDAQ, Yahoo, Google, RAND and other think tanks, Amazon, the U.S. Chamber of Commerce, The Washington Post, usually by attacking infrastructure computers etc., some affecting the systems to the point of "denial of service".

The methods are monitoring, forging, interruption, blocking, eavesdropping, watching, following, electronic chaff, misinform, feint, conceal, change addresses, implement propaganda. There were more than 100.000 cyber attacks in 2009. Google and other information services will cooperate to secure access and service.

.



In June 2009, Secretary of Defense ordered the creation of a US Cyber Command (CYBERCOM) with its headquarters in Ft. Meade, MD. CYBERCOM will operate under the guidance of NSA and the unified command USSTRATCOM and technological support from the Defense Advanced Research Projects Agency (DARPA).[61] Attacks will come from hostile governments, private hackers and crooks. Their motives are offensive, thrill, disrupt networks, create problems, steal know-how, patents, forge information etc

CYBERCOM will organize and coordinate cyber protection and will recommend better operation of the computer networks of the Department of Defense, but also will recommend such procedures to other US departments and agencies. CYBERCOM will also attack foreign and hostile cyber systems and attackers.[62] The current plan seeks to infiltrate stealthy such networks and cut them off the Internet when needed (*Dominant Cyber Offensive Engagement Program*). The overall strategy will be distributed in the fall of 2010. See also: *The Comprehensive National Cybersecurity Initiative* (CNCI), National Security Council, The White House, March 2010; Homeland Security Presidential Directive 23 (NSPD-54/HSPD-23); Air Force Doctrine Document AFDD 2.5.1 *Electronic Warfare*, Army TRADOC G2 Handbook No. 1-02 *Cyber Operations and Cyber Terrorism*, Rebecca Grant: *The Rise of Cyber War*. A Mitchell Institute Special Report, Air Force Association, Washington DC, 2008. etc.[63]

Accordingly to the new CNCI, the White House sees 12 Initiatives: A Federal Enterprise Network with Trusted Internet Connections; Deployment of Sensors to Identify Intrusions; Intrusion Prevention; Research and Development Efforts to Improve Security; Connection of all Federal Networks to Enhance Situational Awareness and Security; Install Cyber Counterintelligence; Increase Security of Classified Networks; Expand Cyber education; Define Technologies, Strategies, and Programs; Develop Deterrence Strategies and Programs; Enhance Security Management of Data and Networks, Enhance Cyber Security Serving Critical Infrastructure.

NATO Cyber War

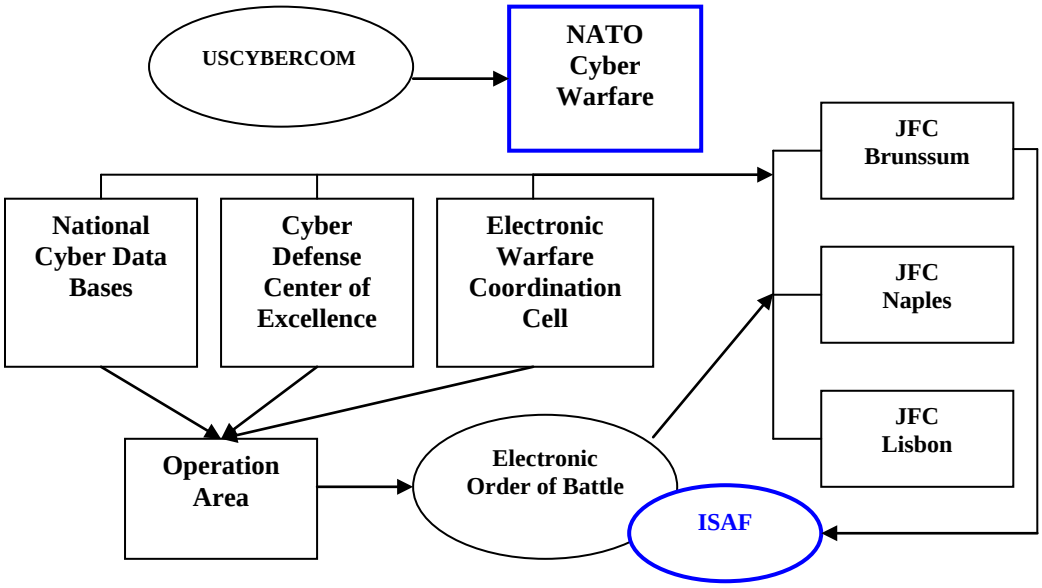
After the cyber attacks against Estonia in 2007 by Russian a government computer center, attacks against the German government agencies from Chinese sources in 2007, NATO had to look into its cyber operations and ongoing attacks.

In May 2008 a number of NATO member states and Allied Command Transformation signed documents regarding the establishment of a *Cooperative Cyber Defense Center of Excellence* in Tallinn, Estonia. In April 2008 NATO decided in the Bucharest Summit to enhance capabilities to encounter cyber attacks against NATO member states.

China attacked NATO information and computer systems during 2009 approximately 100 times a day. NATO was even forced to cancel intelligence and sensitive information via computers to prevent possible Chinese access to such data. NATO has now sealed off its secure Intranet and this is totally separated from the www.

NATO intelligence reported that high ranking members of NATO staffs were socially observed by hacking their Internet, letters with sensitive or content was mailed under disguised names and these individuals were later on blackmailed.

Besides the center in Tallinn, United Kingdom established its own Office for Cyber Security Office in London working with M5 (Director General Jonathan Evans). There is no intelligence sharing between NATO and EU, and UK had to separate its operations to avoid any data sharing with EU.



Structure of NATO`s Current Cyber War Organization. Like in Intelligence, NATO Depends also in Cyber war on National Support

Current NATO Computer Networks and Formats

NATO began in the late 1990s to look into computer assisted intelligence programs and such programs were developed besides operational programs. NATO established a Intelligence *Collection Coordination and Intelligence Requirements Management Cell* (CCIRM, with army, navy and air force sub-cells), which collects all incoming intelligence reports from friendly sources and also structures intelligence requirements for NATO missions, and is sending such requests to friendly intelligence agencies for replies. NATO is organizing its intelligence requirements through the NATO *Special Committee*. U.S. sources point to the fact that NATO is assessing too much tactical intelligence from office desks whereas U.S. forces see tactical intelligence rather as a product of combat, and use such information quickly, because the value of information dominance decreases every minute. NATO decided in November 2002 to improve intelligence capabilities, but much of the problems remain.

European military organizations have no global capability and tailor their intelligence according to their national defense and assumed areas of intervention. Additionally, in the filed of intelligence, U.S. mainly cooperating with Great Britain; within NATO, a number of states for certain reasons do not receive regularly intelligence data. Reasons are political, different software and build-in classification barriers. On the technical level, NATO standardized a number of formats to structure and to disseminate intelligence data (see also AIntP-3 *The Military Intelligence Data Exchange Standard*): [64]

Joint OPS INTEL Information Systems (JOIIS):

It provides all military data like hostile weapons, airfields, facilities, organizations, forces, targets, military hierarchies and key personalities on a global scale.

Battlefield Information Collection and Exploitation System (BICES):

It supports intelligence on the tactical level (see STANAG 4559, 4586).

Electronic Warfare Management System (EWMS):

It gives the EW staff options in fighting enemy EW activities (see ATP-47).

Multifunction Information Distributing System (MIDS):

Tactical data distribution (see STANAG 4586).

Multinational Battlefield Information and Exploitation System (MBIES):

It provides nearly real-time intelligence data to NATO forces.

NATO Imagery Transmission Format (NITF):

NITF supports different software systems used by NATO member-states (see AEPD publication series).

NATO ISR Interoperability Architecture (NIIA):

Interoperability formats for NATO members operating ISR systems, mainly used by air forces.

Request for Information Management System (RFIMS):

RFIMS is part of the CCIRM, and manages *Requests for Information* (RFI) intelligence requests-needs from forces deployed and member states.

NATO All Sources Analyst System (ASAS):

Event-oriented information system, covering specific states and regions, political, military (army, navy air force) intelligence, collected and provided from all available sources.

Imagery Management and Reporting Tool (IMART):

This format provides available imageries and transmits such pictures into its standardized *Image Library* formats.

SIGINT Analyst Functional Environment (SAFE):

NATO obtains signal intelligence from various sources and SAFE is a structure to store and retrieve such intelligence.

Other programs developed and available for NATO are *Locally Employed Personnel* (LEP, which is also available for EU Forces), *Tool for Operation Planning, Force Activation and Simulation* (TOPFAS, a top-down planning program for operations, based on the AJP-1), *Land Command & Control Information System* (LC2IS, supporting commands), *Allied Commands Resource Optimisation Software System* (ACROSS, a logistics planning tool), *Allied Deployment and Movement System* (ADAMS, airlift, sealift, land movement planning), *Effective Visible Execution* (EVE, lists all forces ready for deployment, deployed or rotation out of an area), *Coalition Reception Staging and Onward Movements* (CORSOM, supervises lines of communication to deployed and employed forces), *Consignment Tracking* (ICTC, controls logistic movements by specific radio codes), *Logistics Reporting* (LOGREP, logistic readiness of forces by collecting data about ammunition, fuel, water, spare parts, other supply).

NATO also created data exchange programs in deployment/employment areas, so the *Combined Enterprise Regional Information Exchange System* (CENTRIX) and others.[65]

Experts working in the NATO intelligence branches complain about lack of coordination, continuous rotation of experts, different computer software in NATO and member states. NATO also offers data to Australia, Sweden, Finland, which are considered as “friendly nations”, but on the other hand, Canada did not participate in BICES as a cost saving move but wants now full access. Many states had given up HUMINT and have now problems to

find the “right kind of people” to reinstate such aims; currently most HUMINT outside the larger member states is plain military observation of activities.

NATO also proposed to be linked to the INTELIPEDIA Intranet system of the U.S. Forces, but many states for the foreseeable future will not obtain data, which have a higher classification status than *Restricted*.[66]

NATO Enlargement

The enlargement of NATO was possible because of the collapse of the Soviet Union and of the Warsaw Pact. The former satellite states simply changed sides. NATO enlargement had a geopolitical and geostrategic impact on all European political affairs, and was promoted by the U.S. Governments after 1992/93.[67] The idea was to contain any future Russian expansion into Central Europe, and this affected the relations with Russia. Russia never understood that the attraction of the U.S. as a “friendly hegemon”, of western values and of democratic institutions, plus the protection by NATO, was for the central and eastern European states preferable to any Soviet/Russian dominance as experienced between 1945 and 1989 and any geopolitical construction to maintain such control into the coming decades as proposed by many European governments in 1990/91.

Recent Russian rhetoric to “rebuild Russia in the borders of the former Soviet Union” is seen by these states as a typical threat to their freedom and independence.[68]

The “National Security Threat List”

The *United States National Security Threat List* includes issues of highest priority: Terrorism, Espionage, Proliferation of Weapons of Mass Destruction and WMD-Threats Against the U.S., Economic Espionage, Targeting of the National Information Infrastructure, Targeting the U.S. Government, Targeting the Defense Industry, Other Foreign Intelligence Activities, Food and Water Security, Transportation Systems.

The DIA structured its list of challenges/threats along the same lines but added specific countries, like China and India.[69] NATO has adopted these threats and tasks.

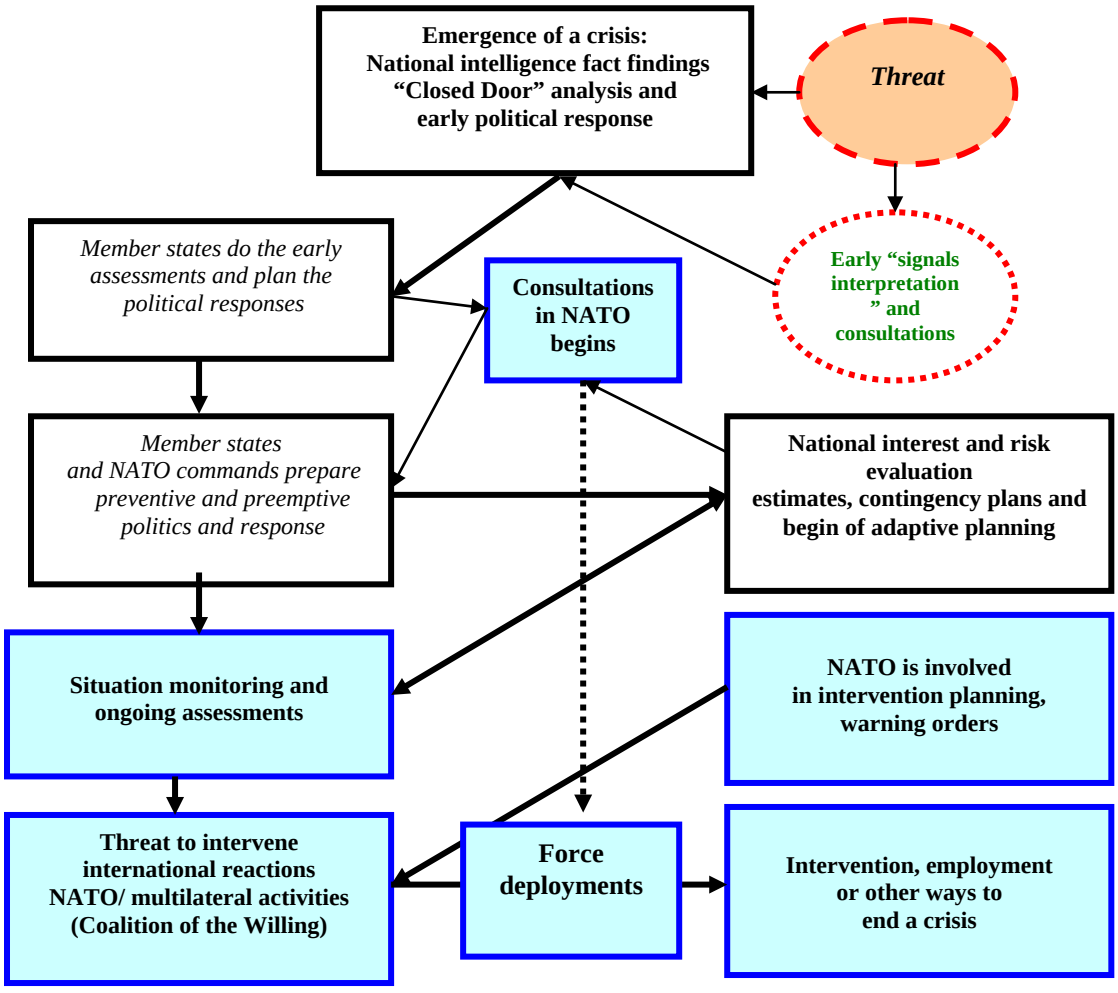
NATO`s Intelligence Organization

A) The Political-Strategic Level

When one talks about "NATO Strategy", there is a distinction between (a) policy and strategy on one hand, and (b) military strategy and strategic operations on the other hand.

Today, the strategic level of NATO is split between the *Allied Command Transformation* (ACT) in Norfolk, VA, which is a force transformation and advisory institution, and the European institutions in Brussels (*North Atlantic Council* and its staffs) and Mons (SHAPE).

ATC is based adjacent to the U.S. Joint Forces Command (USJFCOM) installation to implement certain U.S. transformation and force developments into NATO. In July 2009, a French admiral became commander of ATC, which has, besides a number of elements in Europe, a staff cell for *Strategic Concepts*, one for *Policy and Interoperability*, and a *Joint Warfare Center* for land, air and sea warfare. Intelligence is debated in the *Intelligence Board*, also located in Norfolk.



The basic functions of NATO intelligence is to support the political and military councils, committees and commands

But the final political and strategic decisionmaking level is on the European side of the Atlantic in the hands of NATO`s *North Atlantic Council* (NAC) and therefore with the

member states. The NAC is the highest political body within NATO, which includes the heads of states and the secretaries/ministers of defense; it has a permanent committee of representatives who meet once every week. Permanent institutions in Brussels are:

- The *International Staff*: It is the staff of the NATO Secretary General, currently with eight offices;
- the *Defense Planning Group*
- the *Nuclear Planning Group.*
- The *Military Committee* (MC): It consists of the Chiefs of Staffs of NATO member states. The MC maintains a permanent representative body of lower ranking officers, which meet every week at least once a month. The MC follows the political guidance of the NAC and implements also decisions of the *Defense Planning Group* and the *Nuclear Planning Group.* The staff of the MC is the
    - *International Military Staff* (IMS) with the *Intelligence Division*.
    - The IMS reports gaps in intelligence to NATO member states and will specify what data should be provided.
    - It has a guidance function for a number of other offices and working groups, like
        - The *Office of Security* (which is responsible for infrastructure and organizational security and safety matters of NATO headquarters installations),
        - *The Special Committee* (that will discuss all aspects of NATO security),
        - *The Intelligence Committee* (which is an advisory board in regard to espionage, counter-espionage and other threats which might affect NATO, but also invites the heads of intelligence agencies of NATO member states to periodic meetings and recommends exchanges of data, especially about terrorist activities),
        - *The Intelligence Warning System and Terrorist Threat Unit* (created in 2000) with an *Intelligence Warning System* (NIWS, which operates the *Terrorist Threat Intelligence Unit* (TTIU)).
        - A *Situation Center* monitors all crisis emerging somewhere on the globe and also handles incoming messages.
        - The *PfP Intelligence Liaison Unit* (ILU), based on the *Partnership Action Plan against Terrorism* (PAP-T); it was recommended by the Istanbul Summit in 2004 and is a forum for information, consultation and data sharing.

The U.S. Government recommended bilateral agreements (in addition to NATO decisions) to bypass any legal or political hurdles and problems.[70] Newer developments include:

- NATO proposed to the EU *Military Command* (Brussels) to seek a better cooperation with NATO, and to overcome the EU resistance to work closer with NATO. This cooperation also would include intelligence.
- NATO established links to INTERPOL and EUROPOL.

- NATO established links to additional U.S. commands like SOCOM, FORCECOM, CENTCOM, SOUTHCOM and AFRICOM.

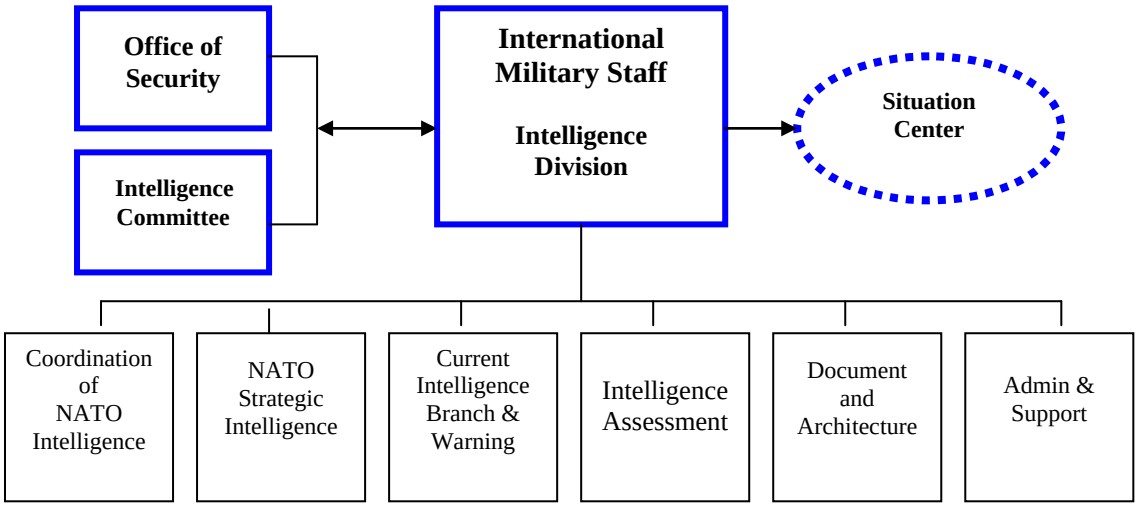
B) The Military-Strategic Level

The Intelligence Division in the IMS

The ID is responsible for all strategic intelligence[71] and estimates, steers intelligence policy, directs digital intelligence bases, and provides intelligence regulations, electronic and administrative formats, and information services to member states. It also performs strategic warning and supports crisis management. It has an

- *Assessment Branch*, a
- *Current Intelligence and Warning Branch* and a
- *Document and Intelligence Architecture Branch*.

It advises the *Military Committee* (MC) and the *International Military Staff* (IMS) in regard of strategic intelligence and other topics, and supports the *Allied Command Operations*. It is also a meeting place of the heads of intelligence agencies of NATO members, and sometimes also hosts such heads from PfP countries.



The intelligence branch of NATO`s IMS is mainly engaged in coordinating the intelligence within NATO member-states and gives strategic warning to the Military Committee and SHAPE/ACO/J2

The ID writes its own assessments, which are distributed to other divisions of the IMS and to the *Military Committee*, and supports the NATO *Situation Center*, the *Defense Planning Committee* and the ACE.

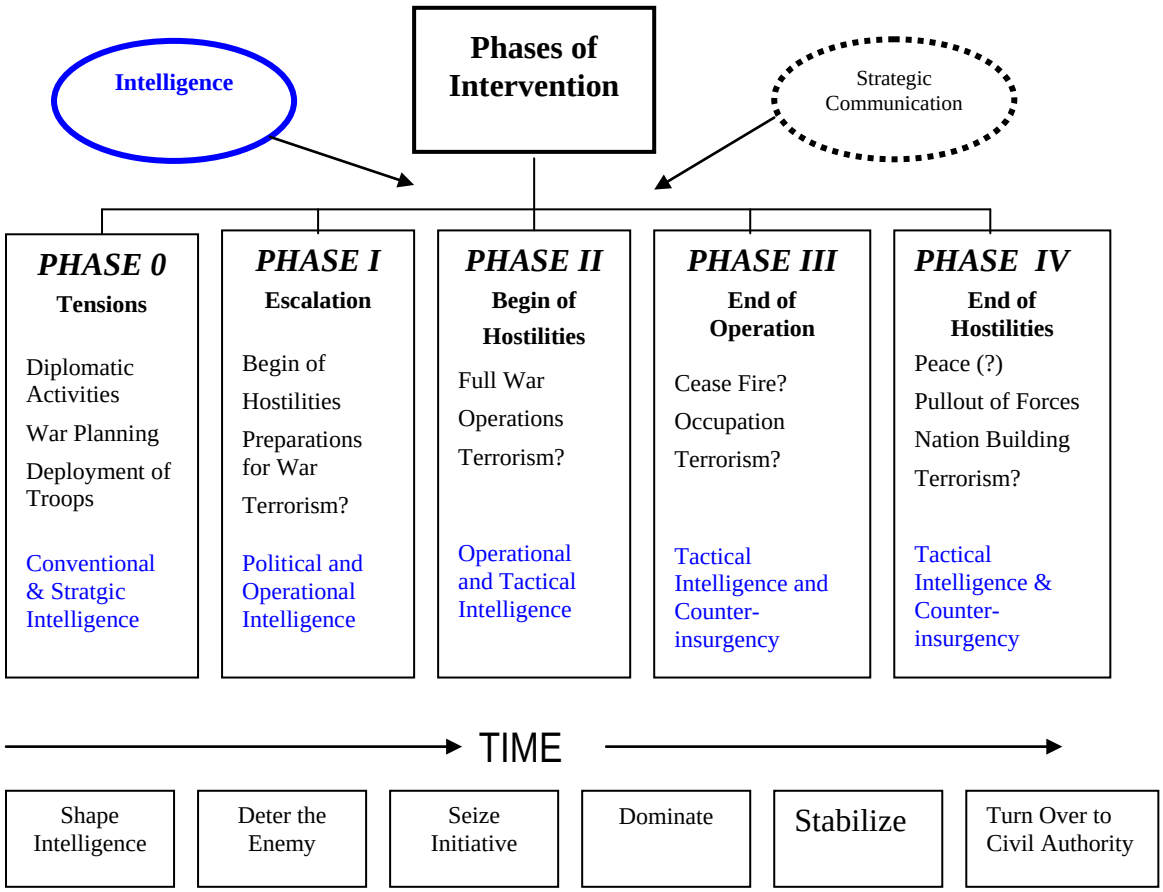
The ID obtains information from the *Nuclear Planning Group*, NATO *Air Defense Committee*, NATO C3A, NATO C3B, NATO *Armaments Directorate*, NATO *Electronic Warfare Advisory Committee*, the EW-*Working Group*,[72] and the NATO *Research and Technology Directorate*.

The Allied Command Operations

Allied Command Operations (ACO), also *Supreme Headquarters Allied Powers Europe* (SHAPE), in Mons, BE, is under command of the *Supreme Allied Commander Europe* (SACEUR), who is double hated as Commander EUCOM.[73] SHAPE is the military strategy-

and also the highest operational level of NATO. (The level of the SACEUR does not separate military strategy and operational planning; therefore there is no difference between strategic and operational intelligence.)

The SACEUR level sees a Deputy SACEUR (UK) and the Chief of Staff/SHAPE/AOC (Germany) which are four-star billets. The staff has (following U.S. staff organization) nine joint staff branches (J-1 to J-9), which are usually found also in operational and component commands, air, land and naval sub-command levels.[74]



Intelligence is required in all phases of an intervention

SHAPE J2

The J2 branch at SHAPE is dealing with military intelligence, and is basically an office to prepare strategic and "operational" intelligence for all kinds of operations which involves NATO, manages incoming and outgoing data and has a role in personnel security affairs within NATO commands. SHAPE J2 has oversight over lower level J2/G2/A2 elements of staffs, deployed forces (joint or combined) and maintains in Mons a *Situations Cell* for computer assisted NATO *Intelligence Domain* data, which provides information for NATO through the already mentioned *Battlefield Information and Collection Exploitation System* (BICES), developed in 1997/98 to serve EUCOM`s PC-based *Linked Operational Intelligence Centers Europe* (LOCE)-system,[75] currently with 2200 users. It is also linked to NATO`s *Fusion Center* and to the U.S. CENTRIX and the Secret Internet Protocol Router (SIPR) net, which is a global U.S. forces crypto circuit-data exchange system.[76]

The J2 also maintains a number of Working Groups dealing with intelligence matters, like estimates, technological trends, intelligence data, communication security, warning issues, special intelligence and sub groups for army, navy and air intelligence issues.

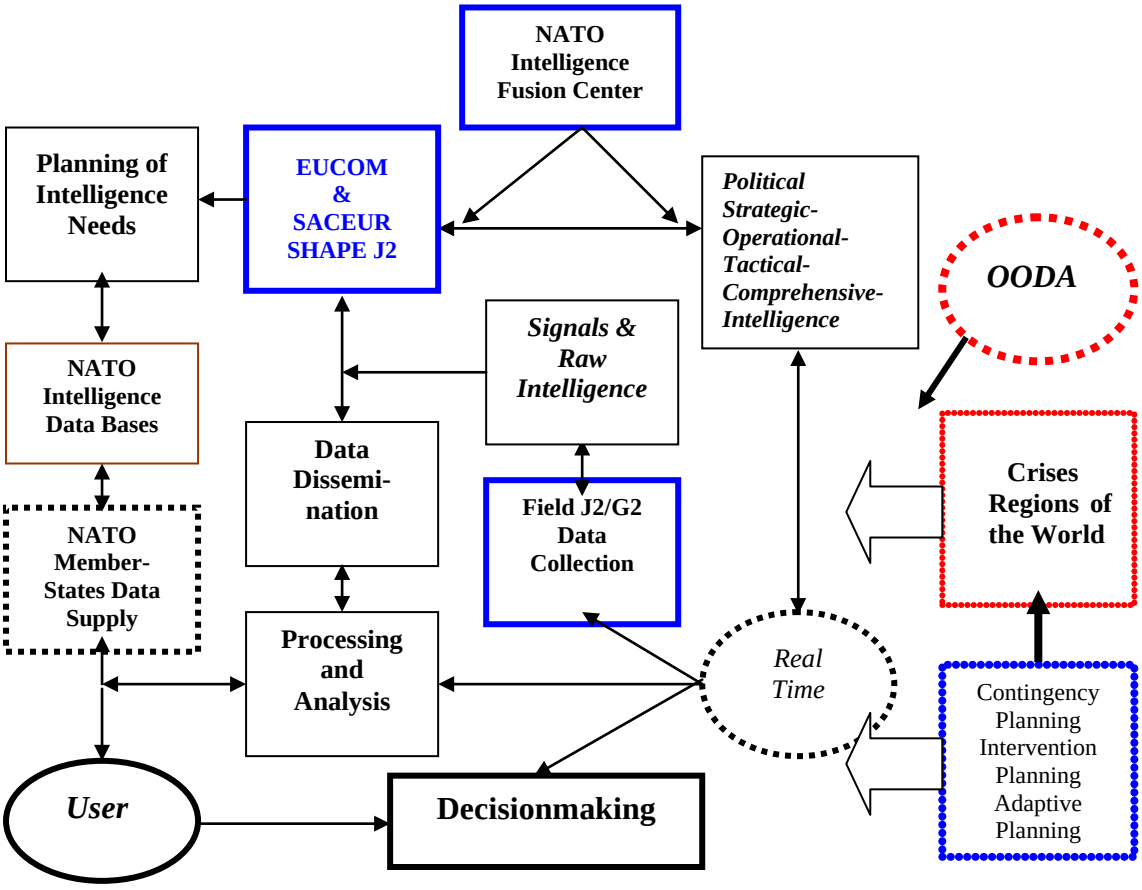
C) NATO`s Intelligence Organization: The Operational Level

NATO maintains three Joint Forces Commands and a number of Component Commands, which are structured along geographic lines, or represent land, air and maritime elements. Each of these commands has a J2/G2/A2 section in its staff. This level is now the keystone for all intelligence support for deployed and employed NATO forces. Employed multinational forces (like in Afghanistan) usually have a joint *Intelligence Center*.

D) The Tactical Level

NATO Intelligence Activities

Even when NATO does not "officially" publish much about its intelligence activities, there are many comments and articles written about past experiences and deficiencies, after-action reports dealing with intelligence problems in the Balkans, Somalia, Afghanistan and Iraq.



NATO intelligence is supported by a number of NATO-integrated and national intelligence agencies. NATO intelligence became important, when NATO began to build up multinational force organizations beside the multinational staffs.

NATO sources agree that most information is easily available, can be collected in advance by overt means, and NATO began a few years ago to mine open source intelligence (OSINT), which provides for 85% of all required data.[77] But commanders in Afghanistan and Iraq need ad hoc/real-time tactical intelligence.[78] Such intelligence is rarely *Strategic Intelligence* but

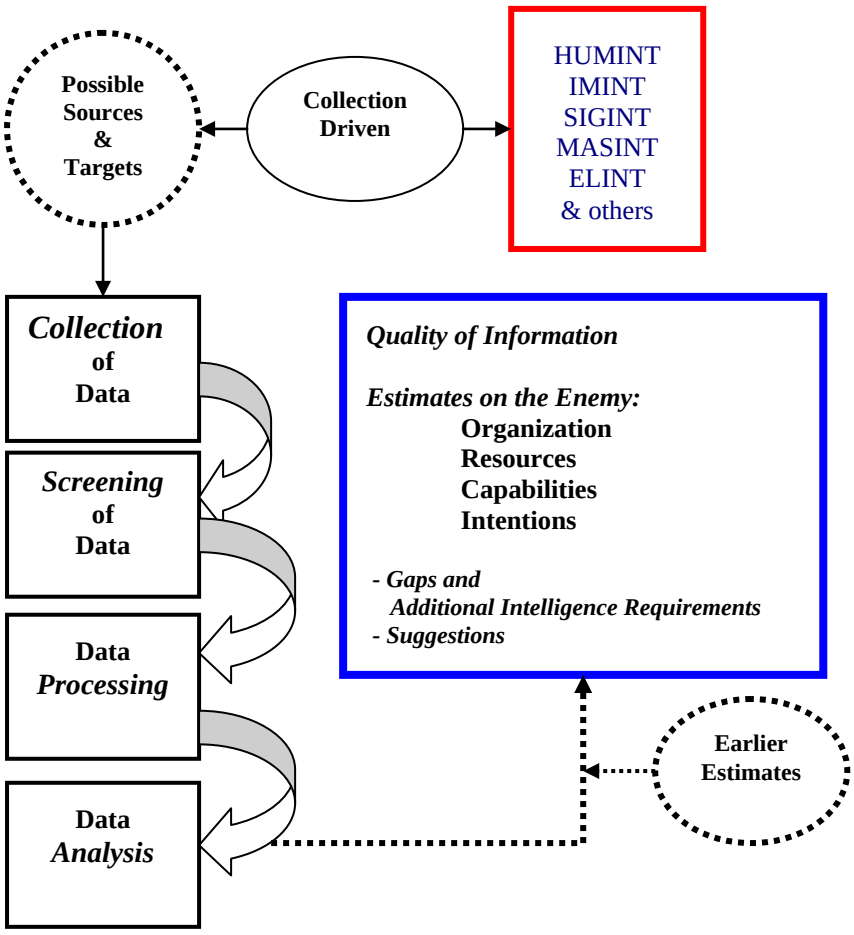
mainly operational *Battlespace Intelligence*, *Tactical (Priority) Intelligence* (”Eyes on Target”), plus (post-combat) *Battle Damage Assessment*.

Intelligence collection still follows the traditional loop of *direction* (what are the issues, often a “strategic” decision), *collecting*, *processing* and *dissemination* (which includes *analyzing*, and *estimating)*, and finally *decisionmaking*, (CPD&D), based on *observe*, *orient*, *decide* and *act* (OODA). Problems emerge at every level: Wrong direction, faulty or missing collection, and failures in analysis, wrong estimates, and lack of proper and quick decisionmaking.

Monitoring Events

One of the largest challenges for any military leadership (in peacetime and war) is the permanent monitoring of events:

- Implement well established knowledge into current estimates,
- look to the future,
- track all possible adversaries and
- never lose touch with events.



The data evaluation process

Each commander will develop a *Commander’s Critical Information Requirement* (CCIR). The J-2/G-2/A-2 will develop a *Commander’s Priority Intelligence Requirement* (PIR).

This intelligence is basically *Order of Battle Maintenance* (ORBAT), which contains traditional military data (Maritime, ground, air, space, logistic etc.) and non-military data

(proliferation, terrorism, environment etc.) reflecting the wider spectrum of NATO intelligence requirements. This data must be available as Basis Intelligence and/or Current Intelligence data. This includes:

- Intelligence Estimate [79]
- Monitoring, Assessment & Prediction
- Indications & Warning
- Basic Intelligence
- Current Intelligence
- Order of Battle Maintenance
- Support to other Warfare Areas
- Target Intelligence

The NATO Nations contribute to this agreed data published by the IMS Intelligence Division. Current intelligence will be maintained by NATO Headquarters/CJTF Headquarters using national intelligence contributions or intelligence collected by forces in or close to the Joint Operations Area.

Within NATO, all intelligence input-procedures are based on the *Collection Coordination Intelligence Requirements Management* (CCIRM).[80] Traditionally, such intelligence collection includes the number of tanks, guns, aircraft, ships, installations, readiness, electronic equipment, technology, large exercises, doctrines and manuals, training, changes in the organizations and the quality of leadership and troops.

The most valuable intelligence is the knowledge of foreign war planning and mobilization data. However, history tells us that such data is often useless. Today, professional forces rarely have the support from reserve structures, and mobilization became meaningless.

Hybrid war also has changed priorities and intelligence gathering. Intelligence, Surveillance and Reconnaissance is now aimed on individual terrorists, individual fanaticism, guerrillas, clans, small communities, social structures, small arms and improvised explosive devices (IED).[81]

Intervention planning is usually based on political and military analysis. The political situation is in most cases well known, but can change quite fast and in a dramatic way, which was seen in Iraq and Afghanistan. Interventions require a pre-deployment analysis of the overall situation, social structures and tactical issues.

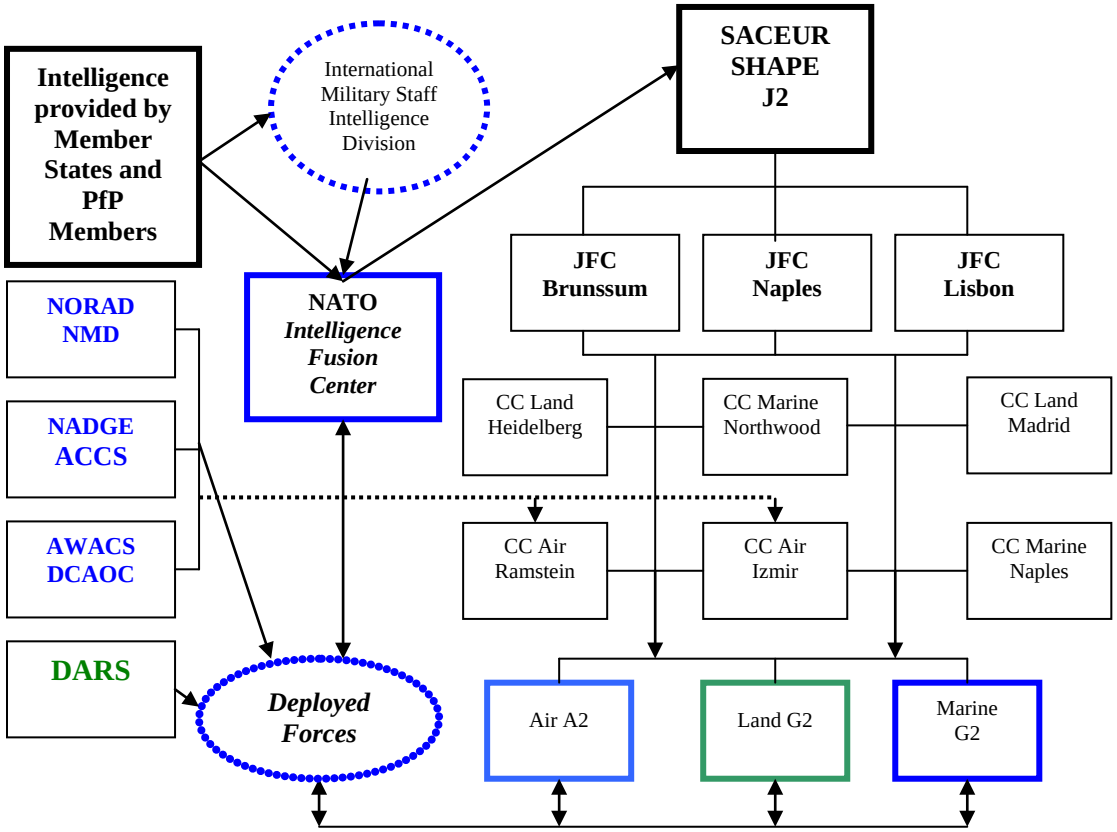
Numerous excellent books were published about global developments, data and many details for judgment.[82] There was a demand on information by state authorities, corporations, investors, banks, retailers, tourist companies and others to evaluate risks and other problems facing entries into such markets.

But in the future, NATO faces other challenges, like political radicals, terrorism, proliferation of WMDs, rogue governments, new state-to-state rivalries, ethnic tensions, state failures, sectarian mass killings, poverty, ineffective governments, urbanization, shortages of energy, local water and food supply, finally environmental degradation.[83]

Staff Work and Intelligence

U.S. allies and NATO forces in Iraq and Afghanistan work in joint staffs or have liaison staffs or teams. Joint staffs require skilled officers and NCOs.

U.S. and NATO officers complained that intelligence data was (and still is) not distributed on time. Obstacles are mainly hardware-based. The U.S Joint Forces Command and NATO`s ATC identified a number of problems.[84]



The Intelligence organization of SHAPE/ACO can also be divided into strategic, operational and tactical levels.

But barriers still exist (a) within the U.S. intelligence community, (b) between U.S. and NATO intelligence and (c) within European intelligence agencies. It is a fact that even national intelligence organizations do not cooperate too well, and, like in the past, act often as “closed shops”.

The typical problems in Iraq and Afghanistan involved intelligence, planning, information security, situation reporting and attack reporting on time, targeting policies, organizational issues, intelligence planning and coordination in the field, prevention of fratricide, logistics & transport planning, network- and hardware-interoperability, and air support coordination. Brigade- and battalion-level planning is often “crash planning”, with tight time-schedules for the planers. Under such circumstances, valuable and new information is often not part of decision-making. Conventional tactical air reconnaissance is still slow, data is not distributed on time etc.: Airborne relay for tactical data is a must.

Tactical intelligence cannot be based on TECHINT only, but must enhance HUMINT information on a person-to-person basis, a process called now “social intelligence”.[85] When in 1977 the U.S. intelligence community was told to collect information mainly by TECHINT means, NATO did not receive any satellite imageries, because they were then considered as “sensitive”. Today, images with excellent resolution (50 cm) can be bought for a reasonable price by any individual via Internet. Exchange of information from one agency to another is often prevented. Therefore, there are intended and non-intended communication-gaps. [86]

E) Counterintelligence

NATO has no integrated operational counter-intelligence, but has an internal counter intelligence/security section, which is providing such tasks inside NATO installations (Brussels, Mons, Norfolk, Naples, Brunssum and so on) and staffs.[87] Most counterintelligence is done on a national level and for NATO by the 650th Military Intelligence Group/*Allied Counterintelligence Activity* (U.S. Army) at SHAPE.

Counterintelligence activities within NATO are based on *The National Counterintelligence Strategy of the United States*, the DoD Directive 5105.67 and FM 34-60 *Counterintelligence*. Counterintelligence is mainly supported by the U.S. *Counterintelligence Field Agency*, which supervises and manages the protection of the Department of Defense (and advises other nations about such protection programs), which includes key personnel, resources, critical infrastructures, critical information, and foreign espionage against the Department of Defense (and NATO).[88]

The United States has a number of laws, which punish espionage: The *Espionage Act* of 1917 (amended in 1950), the *Internal Security Act* of 1950,[89] and the *Atomic Act* of 1954 and now the *Patriot Act* (as amended). NATO, as an international organization, depends legally on national laws and rule-enforcement.

F) The Administrative and Procedural Level [90]

Sharing of Intelligence – Obstacles Remain

NATO intelligence is guided by the AEDP series of publications, the ATP-47 *Handbook for Air Reconnaissance Tasking and Reporting,* some 40 STANAGS,[91] C4ISR,[92] C4ISTAR[93] architecture, Data Link procedures, plus guidance of the J2 work,[94] regulations for interconnected computer software that is handling sensitive intelligence data, like CRONOS or the Maritime C2 Information System.[95]

Administration also guides (accordingly to political and military decisions) the distribution of intelligence data to member states and PfP-states.

There is still a national and agency tendency to keep information "in-house".[96] The reasons for not sharing data are either personal, "group think", political, organizational (policy), lack of mutual trust, or structural.[97]

But over the last years, NATO has collected a tremendous amount of intelligence data. Handling of such data is now organized in a number of computer-/software-formats. If, and with whom, such data is shared, is based on a "need to know" policy.[98] Also there is a need to prevent security breaches.[99]

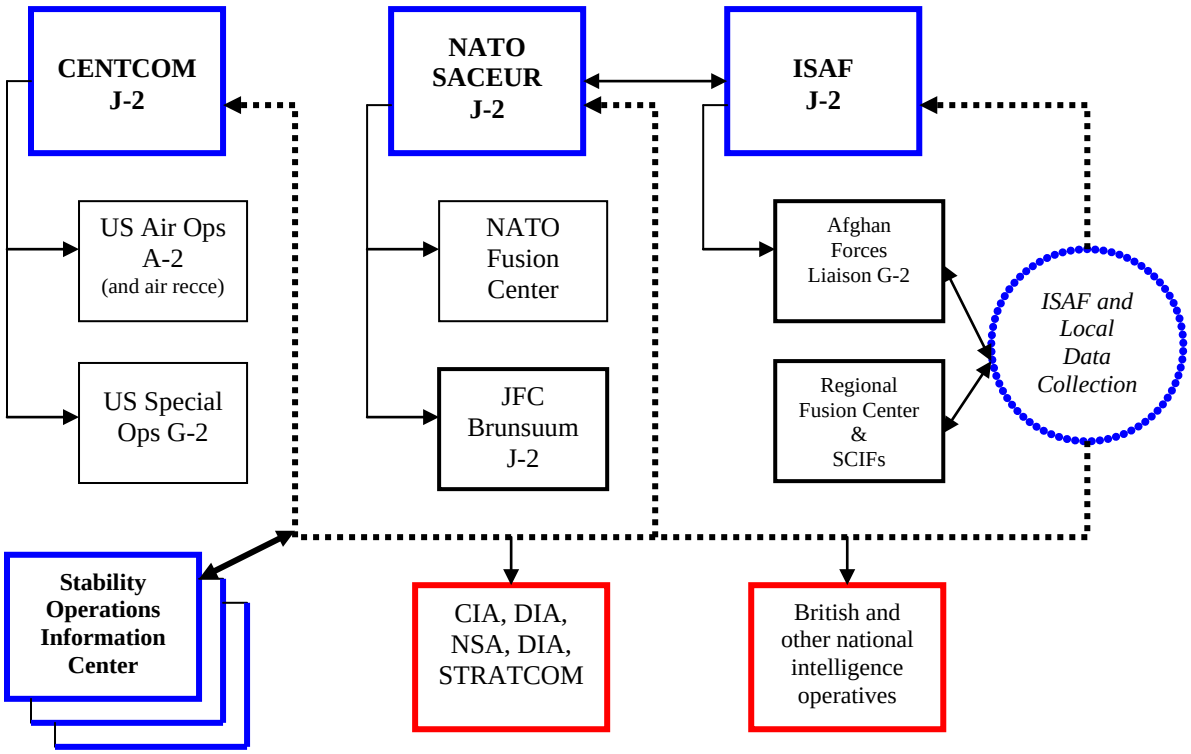
Typically, U.S. laws can limit such access.[100] And because U.S. regulations are implemented in NATO regulations (because different standards in the United States and in NATO would otherwise undermine the common classification of documents, standard procedures and oversight) other countries also act similar.[101]

Additionally, there are specific agreements between Washington and London, Washington and Bonn/Berlin, and so on. U.S. and NATO have provisions for registry, security clearances, protection of information and about specific equipment and armament. NATO`s *Office of Security* delineates what will be included in such agreements with member- and PfP-states, and in each state one agency is responsible for maintaining the agreed security standards.[102]

The exchange of information became a necessity when NATO began to operate in the Balkans and especially during *Operation Allied Force* in 1999, when U.S. forces and other participating NATO air forces had different target lists and intelligence estimates. For

Washington it was too burdensome to explain to European governments why specific targets had to be bombed. Data exchange became a must after the war of 1999.

In Iraq and in Afghanistan, U.S. and NATO-staffs realized that many members of the *Coalition of the Willing* did not possess adequate intelligence data and intelligence equipment, like satellite communication sets. On the other hand, especially U.S. intelligence agencies complained that other NATO members would not share their data. U.S. had to convince member-governments to "improve" this situation.[103] Some European governments openly dismissed U.S. political aims and targeting and preferred "soft" solutions.



There are three quite independently acting intelligence structures operating in Afghanistan, with three separate networks in the country and different lines of communication (CENTCOM, NATO, ISAF). Additionally, the U.S. intelligence community and other national intelligence organizations are also present. There was until February 2010 no joint point of contact for all intelligence gathered. Now the new *Stability Operations Information Centers* were established in each ISAF region and each brigade headquarters.

Protecting NATO`s Interests and Secrets

Classification of Documents [104]

Classification of documents was also changed and simplified. (Top Secret, Secret, Confidential and Classified). Additionally, unclassified information can be seen as "sensitive" or as *Controlled Unclassified Information*. Personal clearances were demanded for all persons with access to NATO *Confidential* and higher. To have access to NATO facilities, a specific clearance is required.[105] Personal involved must be given a security briefing and the persons must sign a form that specifies security requirements.

All classified NATO documents are the property of NATO. Only NATO can declassify or downgrade documents; declassification requires the consent of the issuing NATO department or command.

Physical Protection of Documents

NATO documents must be stored in specified containers; only NATO *Restricted* can be stored in locked cabinets, bookcases or desks, Confidential and higher must be stored in vaults or safes.

Protection of Information

Intelligence includes the protection of plans, information, weapons etc. Some sensitive issues like high–resolution imagery of military installations, ships, tanks, antennas, nuclear power plants and so on, are now published in books, or imageries can be bought from commercial satellite companies. Other problems are cased by lax security measures or simply when such information is not protected, as one would normally assume.

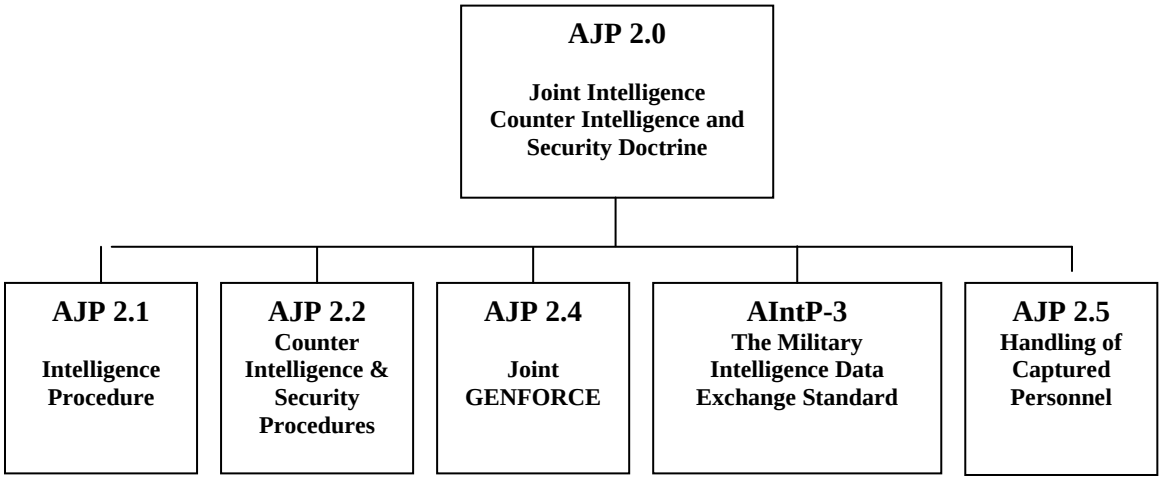
A very recent case was an aerial photography of a nuclear submarine of the *Ohio* (SLBM) class, which was sitting early in 2007 in a dry dock in Bangor, WA, with the driving propeller fully visible.[106] The propeller of a nuclear sub was considered as "Top Secret", and was never shown on any photograph. An expert can calculate speed and other boat characteristics simply by analyzing the screws. The question remains why a civilian aircraft was permitted to fly above a nuclear submarine base, why the crew could take pictures, why this pictures were published on the Internet by Microsoft, and why *Google* afterwards did not immediately block the access to this picture.

Sensitive information includes detailed force relocations and tactical employments, research and development, C4ISR/C4ISTAR, improvements weapons, radar war-frequencies, locations of listening posts, equipment-purchasing, public diplomacy activities. Leaks, like e.g. in the U.S. from government departments to mass media,[107] or from Congress members to mass media can have a severe impact on security.[108]

NATO must look to the impact of detailed information, regarding interventions, international operations, and other plans, when one can derive sensitive data on national foreign policy, national internal security policy and other information, which is often available on the Internet.[109]

Allied Joint Publications on Intelligence (AJP 2-series)

NATO adapted in 2003 the new US modules of manuals and joint publications. This resulted in the intelligence field to a number of publications:



An Independent European Intelligence Organization?

The European Union discussed since 1995 an independent CIA-like organization, and the Military Staff on the EU recommended a DIA-like structured military intelligence organization.[110]

Especially small EU member states hoped to have access to information from the large national intelligence organizations, and to sit as equals on the table of a European intelligence community. The idea, embraced by President Chirac again in May 2000, included OSINT, clandestine operations, access to the space data (Satellite Center, Torrejon, Spain), early warning, the overall situation picture, counterterrorism, but also civilian intelligence which would include diplomacy and other sources.[111]

The idea was dropped because a fully independent autonomous military intelligence agency, totally free from any connections to national intelligence organizations and NATO intelligence as well (already doing such work), remained a strange proposal, even after it became part of the Amsterdam Treaty of 1997, of the 1999 *Cologne Declaration*, and was finally discussed to support *Petersberg* missions (as decided for the first time in June 1992). The issue became debated again when the *Headline Goal* proposed the *Rapid Reaction Force* (an intervention force) was pushed by France.[112]

But, how will NATO intelligence be prevented from being used by EU staffs? The U.S. and Great Britain insisted on a clear separation, which is impossible to accomplish. Doing just OSINT-intelligence alone, would not justify such an independent EU-intelligence organization.

The issue came up again in August 2008, when the French EU Presidency convinced Germany to look again into this matter and proposed a somewhat smaller organization headed by the already existing EU *Joint Situation Center* (SITCEN) in Brussels, acting as a small EU *Intelligence Coordination Center*.[113] This center should, so the idea, combine intelligence, DNA data, fingerprints, surveillance camera data, electronic listening posts, satellite imagery, UAV imagery and other materiel. Again there is opposition from many sides, including Great Britain, and there is the danger that such data would end in some “wrong hands”, when distributed to certain “less reliable” EU members. (NATO itself, on a “need to know”-basis, is not distributing sensitive intelligence data to a number of its own members.)

Final Conclusions

NATO Gets Better Intelligence

Representatives of NATO argue for an increase of NATO operations "out of area",[114] but complain about the limited or even lacking intelligence capabilities of the member states, lack of cooperation, inadequacies in interoperability, national blockades to share intelligence, lack of funds, "soft" approaches in foreign policy and military strategies, no financing of important programs like ISTAR, satellites, software, and aerial reconnaissance, and a leniency when it comes to encounter Russian, Chinese, and other hostile intelligence activities in the west.

Interoperability is the key to NATO success. Much has been said and written about this issue and a number of NATO summits, committees and decisions dealt with interoperability.[115] Many see procurement anarchy, despite tight budgets, plus technology gaps between the U.S. forces and European forces that leads to an even wider divergence within NATO.[116] But such divergence is also present within the EU – no wonder, because the involved governments are identical.

Much was said about NATO transformation and intelligence improvements but intelligence remains still a national prerogative. Intelligence hardware is neither NATO- nor EU-driven, but mainly U.S. driven, industry driven (new technologies), threat-driven, and now counter-terrorism-driven. National priorities remain: There are some 60 different UAV programs financed in NATO-/EU-member states, but there is no plan to concentrate all efforts on maybe five or six systems, which would make sense and save money for other projects. Cost drivers, like real-time sensor systems, data link or encryption equipment, are often national programs, based on national research policy and jobs involved. Most European governments have preferred to invest only limited resources in mass migration control, but next to nothing to combat organized crime; counter-terrorism is seen as a police function.

There is a Revolution of Military Affairs - also in Intelligence [117]

RMA is described in numerous books and articles. RMA is connected to terms like "Shock and Awe", "War of the Third Wave", "Fourth Generation of Warfare", "Transformation of Forces", "Military Technological Revolution", or "Revolution of Military Warfare".

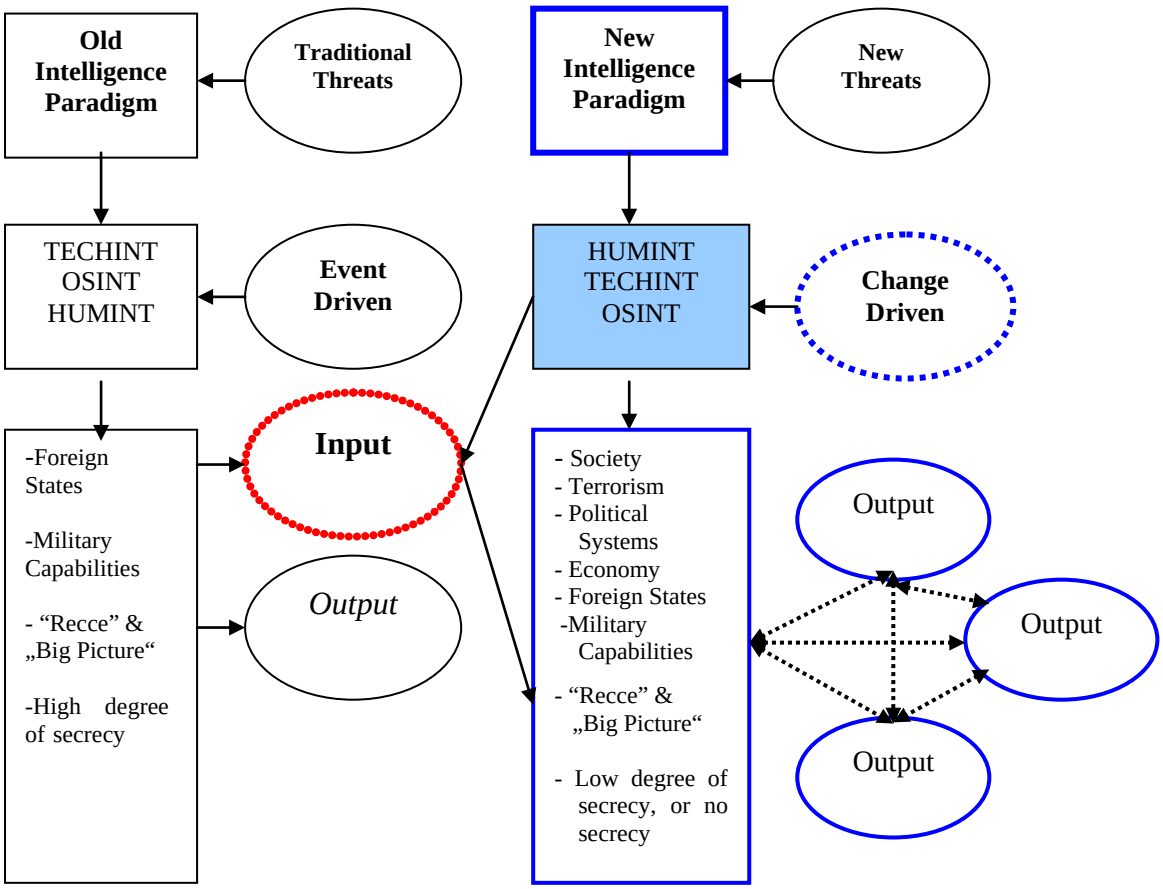
TECHINT, ELINT, Cyber War-systems, GPS and J-STARS had a tremendous impact on intelligence, so had AWACS and new Data Link systems and BVR weapons on aerial warfare. Communications provide real-time situation-pictures of high value and authenticity. GPS provides pinpoint accuracy in targeting. C4ISR/C4ISTAR system merge sensors, communication and information, provide quick inputs and outputs, based on Data Link and other networks, combine reconnaissance and surveillance, satellites, aircraft, helicopters and UAVs. The interpretation of images is partially automated and electronically analyzed. Synthetic Aperture Radar (SAR) has helped to improve the quality of pictures. Supporting equipment helps the analyst to identify targets even when only fragments of a target can be seen or a blow up of a photo would only provide blurred images.

There are Limits to Intelligence

The limits to intelligence are well documented and involve political and strategic assessments and ground, naval and aerial warfare issues alike.[118] What is supposed to be known, but in fact is not, can have dramatic consequences. What is true for operations is also true for intelligence: Intelligence data have a short life-span.

If the intelligence community depends on information of questionable sources there is always a danger of being "wrong". "Citation cartels" can contribute to the danger that vague assumption become "true", because errors if they are reported by many other agencies will be believed.[119] Also, many analysts follow their own bias and preset determinations.

The mindsets of the intelligence analysts, and the expectations of decisionmakers, might be different, but decisionmakers will blame intelligence for their own wrong assumptions, or will blame intelligence for not predicting exactly what will happen, even when events were clearly outside of possible or rational forecasting.



The change from the Cold War era to the new paradigm required a new approach to leadership and organization to master the new threats and requirements. The U.S. experienced such changes of paradigms after Pearl Harbor, the Soviet A-bomb and the Soviet and Communist threats, the end of the Soviet Union and Warsaw pact and finally "9-11". Such transformations require internal transformations, which need ten years and longer. Was HUMINT mainly replaced by TECHINT, HUMINT is now again the most crucial element of intelligence.

Intelligence might come to wrong conclusions: Group thinking, following traditional judgments and perceptions which proved to be right many times before, can be the reason for a totally wrong assessments - and that with a dramatic outcome.

Intelligence must simplify complex situations, or fill in with their experience when only fragments of a (possible) new development are known. The typical problem of *weak signals*-interpretation is its lack of a clear indication what is really happening, why, when and how.

Wrong interpretations or the inability to place such information into a "picture" is quite normal. Information that seemingly fits exactly into fixed expectations, can lead to logical, but notwithstanding wrong conclusions. And there is always the limit on manpower; staffs are swamped with data.

Surprises Will Happen

One must accept that occasional surprises will happen.[120] It is not part of human nature to expect always the worst or the non-expectable and even experts and governments can come to wrong conclusions. Additionally, besides wrong intelligence, available correct intelligence is often disregarded either by politicians or by military commanders.

Analysts are embedded in the mainstream of thought, might be caught in their own cultural views, and decide following rational predictabilities. Surprises will happen if they occur outside of such logical parameters.

The impossibility to predict long-term developments is well known (and especially useless as seen in regard to economic developments), but even when contradicted to logic, there is a hype for such “futurisms”. Typical is the desire to have experts looking to developments for the coming 10, 15 or 25 years, composing predictions, which are quickly outdated by unpredicted events.

Prevent Politicised Intelligence

The problem of politicized intelligence is a permanent issue and not a new one.[121] In the U.S., the CIA and military intelligence identified vs. the Soviet Union a submarine gap, army division gap, bomber gap, tank gap, missile gap, space weapons gap, intelligence gap, manpower gap, and so on, but these gaps were rather quantitative. US forces were better trained, of better quality and maintained a higher readiness rate.

Vague considerations of remote possibilities for the next decades (like the beam weapon-imagination of the early 1980s) gained momentum and became then an imagined threat to national security. Iraq is another case, were the history of a sophisticated WMD-program led to the (partially correct) conclusion that Saddam Hussein started such a program again after 1993, but there was no such program after 1998.[122]

Use a combination of *HUMINT, TECHINT, OSINT*

HUMINT, TECHINT and OSINT, are complementary. They support findings and help to avoid errors, especially when providing overlapping information.

Much was written about satellite reconnaissance, but rarely were the limitations of such platforms explained clearly to politicians or the public: Only the topographic surface of the earth can be monitored, and even IR-sensitive film has its limitations.

Electronic surveillance will not intercept voices or data not transmitted by signals. Even electronic signals (SIGINT) are often encrypted, open communication will use innocent code language, and the overload of messages will delay dissemination and the identification of imminent dangers. Much information is intercepted but is not or too late processed. True, HUMINT often will only provide small puzzles of a still too vague picture, but it can be the only one and the decisive information.

Data Link, Downlink Security, and Limits to Communication, Internet

Frequency overload and jamming is not a new problem, but radio, data link, computer network-security etc. are a problem for frequency management and electronic combat communication.

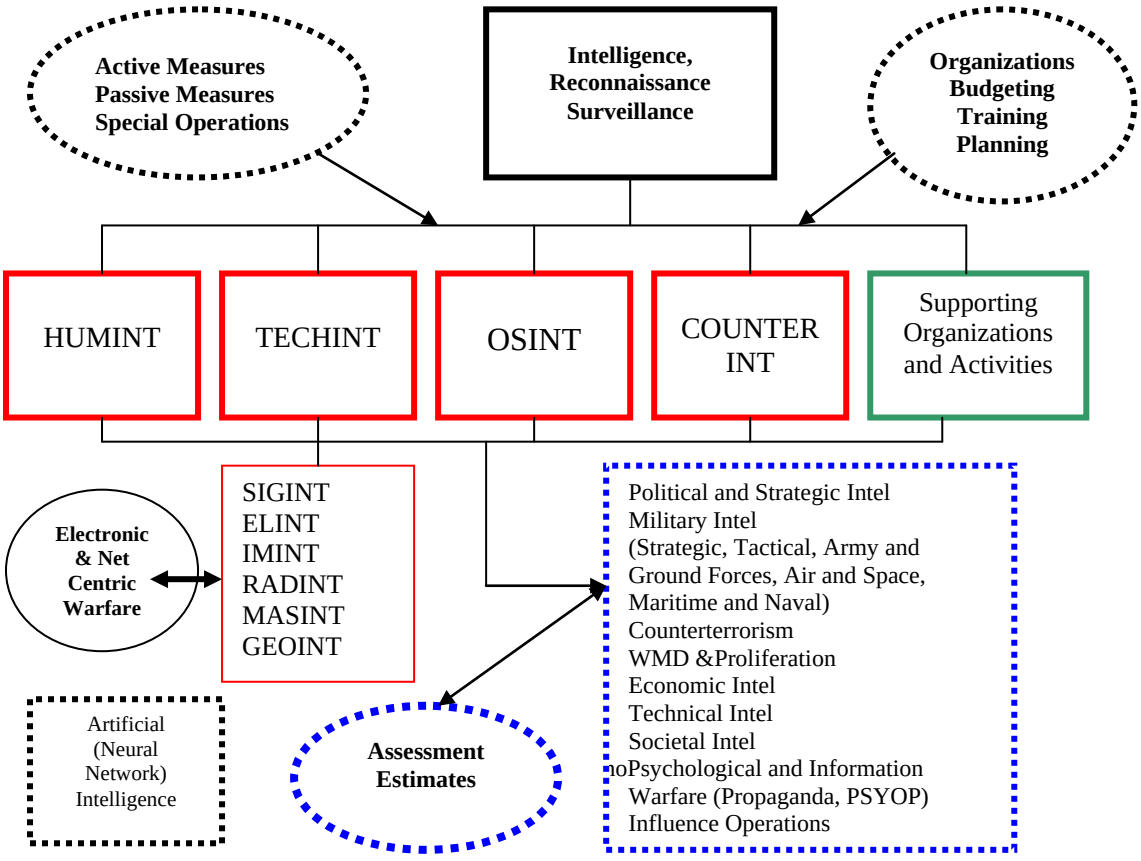
UAV downlink can be intercepted. Internet can be manipulated, and high dependency on Internet might backfire if such frequencies are jammed or intercepted or become a tool of hostile counter-intelligence.

Artificial Intelligence Rarely Works [123]

In the 1980s it seemed that the final answer to all intelligence problems was found in *Artificial Intelligence* (AI). The reason for this was the lack of precise forecasting, different assumptions, the uneasiness with HUMINT, and political implications, especially when friendly governments were "subjects of interest". Many think tanks, universities, and agencies, developed various AI-solutions and vast amount of literature described AI-methods.

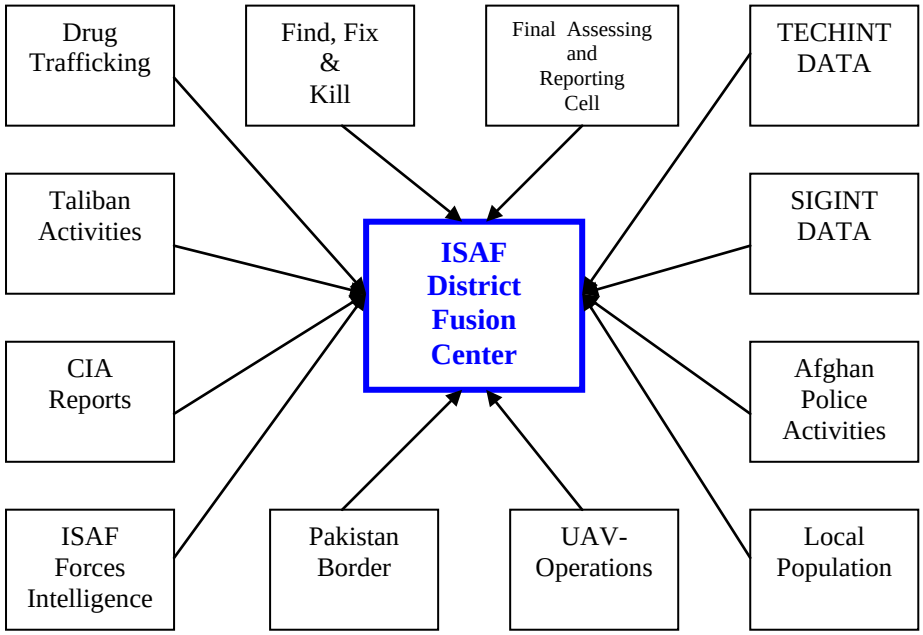
When computers became more sophisticated, also specific AI-software offered solutions: If certain events and little information and hints would be combined - so the ideas in the AI-community - other disguised events would be identified, even if not observable. Chains of events would lead to specific situations if fed regularly into computers and such a process would create better insights and better estimates.

But the results were disappointing: In reality, computers and software would only permit a limited number of inputs. The experts had to choose what they would consider as case-related or relevant to the most probable outcome (but such they could do without computers as well). The main problem of AI was the quality of raw data, which was mainly based on newspaper-reporting, press releases, and commercial radio intercepts. AI simply duplicated what media and the diplomatic service would report anyway. There were no additional gains.



NATO has only a small intelligence organization, but does intelligence training for its members and PfP-nations. NATO has no independent HUMINT and TECHINT, but collects OSINT data and is supported by other (national and NATO) organizations. NATO operates a multinational structure within air defense (NADGE) organization and AWACS. However, NATO does "active" intelligence (HUMINT, TECHINT, COUNTER INT) in the Balkans and in Afghanistan.

AI had to combine news, diplomatic information, data on politics, economy, technology, social affairs, military information, internal events etc. But how would a specific event in one section affect other sections? How would different processes correlate? Grading of events on a scale from one to ten should help to pinpoint possible troubles but such grading depended on the subjective judgments of operators, which lacked often knowledge of a particular region or country, its language and culture, and such grading is always guesswork. Bringing in experts was one solution, but knowledge would not overcome the barriers of software-limitations. Additionally, AI was useless to fight terrorism.



End "National Tactical Data are Nobody's Business" Attitudes

US intelligence officers and ISTAR experts complained over the last years that contingent commanders and staffs keep intelligence data as their "private property" and do not share intelligence. This is also true in regard to national special forces, TACRECCE, SIGINT, and HUMINT. There is still no fully operational ISTAR in Afghanistan and neither software nor data link lines are currently able to handle ISTAR full motion video-data if available late in 2010.

The Current Main Problem: An Afghanistan National Forces Reliability Deficit

Recent intelligence reports indicate a low reliability of Afghan forces and police. Allied intelligence is now putting their attention to the National Afghan Army and contacts of officers and NCOs to Taliban insurgents. Police was frequently involved in cooperation with attacking Taliban forces, drug trade and large-scale bribery. Police may have joined Talibans and Talibans may have infiltrated police and Afghan intelligence.[124]

A New Age for Intelligence: The *Flynn Report* and the *Center for a New American Security* Paper

MajGen Michael T. Flynn, J2/CENTCOM, Cpt Matt Pottinger, USMC, and Paul D. Batchelor, DIA were sent in November 2009 to Afghanistan by order of Gen. Petraeus, CGCENTCOM. Their critical report was presented to Gen Stanley McChrystal, Gen Petraeus, the Department of Defense, and was published in January 2010 by the *Center for a New American* Security, a Washington DC think tank.[125]

Flynn complained about a wrong understanding about the tasks of intelligence, too much emphasis on strategic intelligence, not much usable intelligence on the battalion and company level, different software and formats, findings were not distributed, national ISAF command do not share their intelligence with other nations or with CENTCOM, a number of ISAF contingents and staffs have no command of the English language, even when this was made a requirement for serving in Afghanistan, not enough contacts with the local population. Flynn also:

„Eight years into the war in Afghanistan, the U.S. intelligence community is only marginally relevant to the overall strategy. Current intelligence practices do not provide high-level decisionmakers the information they need to wage successful and, ultimately, the knowledge the need to wage counterinsurgency. Intelligence has devoted too much effort in targeting insurgents and too little analysis…" [126]

Some of Flynn's comments were not welcomed by Defense Department officials (so Pentagon Spokesman Bryan Whitman). However, the Undersecretary of Defense for Policy, Michele Flournoy, assisted Flynn when she said that intelligence is

"ignorant … and disengaged from people in the best position to find answers." [127]

Flynn had toured Afghanistan with two DIA officers. What they saw had fully acknowledged earlier complaints: Sloppy data collection, no contacts to the civilian population, ISAF national forces have language problems to communicate with US staffs or when reporting incidents, there is no transmission of data, different computer systems and formats prevent exchange of data, sent data is not found because of sloppy data handling, and the Taliban have learned to infiltrate between ISAF-areas of responsibility. Flynn ordered the establishment of *Stability Operations Information Centers* (SOIC) for each brigade or ISAF region.

Intelligence has moved away from fixed parameters (numbers, organizations, borders, technical capabilities) into non-fixed parameters like movements of peoples, political radicals, religious fundamentalism, potential terrorists, bribe, weapons and explosive smuggling, mobile phone conversation etc. General McChrystal:

"Our senior leaders – the Chairman of the Joint Chiefs of Staff, the Secretary of Defense, Congress, the President of the United States – are not getting the right information to make decisions … The media is driving the business. We need to build a process from the senor all the way to the political decision makers."[128]

Petraeus, McChrystal and Flynn reminded the forces that in Afghanistan all intelligence is political, strategic, and tactical at the same time; there is no clear distinction between these. Flynn also changes a number of methods, which evidently did not work in Afghanistan:

- Select teams of analysts empowered to move between field elements to visit collectors of information at the grassroots level and carry that information back to the regional command level.
- Integrate information collected by the civil affairs officers, PRTs, Afghan liaison officers, NGOs, UN officials, psychological operations teams etc., and the infantry battalion level.
- Information should be separated by geographic lines not functional lines.
- Write comprehensive (low level) district assessments, not large area (province) assessments,
- Install "information brokers" at regional command level who will provide proactively and on request all data reported and collected in newly established *Stability Operations Information Centers*. The staff working in such a center must be open minded, energetic, and bright.

- Increase the intelligence staffs at battalion (S-2) and brigade levels (S-2).
- Combine HUMINT, SIGINT, TECHINT information and *Significant Activity Reports* (SIACT).
- Look out for insurgents and strike where it hurts most but do not devote all the time to such tasks, look for better governance and fight corruption.
- Operate along the strategic aims of ISAF. Avoid reporting at length in summaries about things and events everybody knows anyway or you find already in newspapers.
- UAVs are valuable but do not tell much about the "tactical climate", mosques attitudes and the bazaar and people's concerns.
- Intelligence begins at the company level. In Afghanistan NCOs doing intelligence work were assigned to company commands.
    - US Army: *Company Intelligence Support Teams*
    - USMC: *Company-Level Intelligence Cell*
    - Battalions should report to brigades, and each brigade should have a *Stability Operations Information Center*.
    - Support *Fusion Centers* at the higher region's level; they have a number of *Sensitive Compartmented Information Facilities* (SCIF) to handle sensitive intelligence data accordingly to specific requirements of higher commands.

  reporting about incidents, IEDs, patrol reports, contacts to Afghans, condition of roads, bridges, weather, drug trafficking, problems in supplying water to the local population, attitudes of women, number of Kalashnikovs, medical support etc. in a daily "Master Report".

  Above brigade level there is no additional gain in relevant intelligence data.

- Killing Talibans will not solve the problems and will only multiply the number of insurgents. The Soviet killed them by the ten thousands and did not win: We must win the local population.
- Support the traditional hierarchies and weaken the Taliban's attempts to strengthen the younger men with the purpose to undermine the elders and win the young men over.
- Reduce the current knowledge-deficit at all levels, do not be passive, avoid the "comfort zone" and share relevant information faster. Information will not fall into your laps: Report findings to ISAF and CENTCOM.

What is at stake? The credibility of the USA, of NATO, of ISAF, the future of Afghanistan and of Pakistan.

> *Intelligence Failures are failures of command just as operations failures are command failures.*
>
> Marine Corps Doctrinal Publication 2, Intelligence, 1997, p 77

Appendix: Definitions of Intelligence (official texts in *Cursive*)

There are numerous and quite different ways to define intelligence.[129] Earlier definitions usually did not contain terrorism or non-state intelligence by private or investigating companies or private analysts who usually do intelligence work for state and non-state clients.[130] Earlier definitions also lack comprehensive and hybrid-war requirements.

According to NATO terminology, intelligence includes also counterintelligence, physical and infrastructure security, and geographic support of headquarters:

Intelligence *is the collection, analysing and dissemination of intelligence information to assigned forces and the headquarters staff. In cooperation with other NATO and National Agencies, J-2/G-2/A-2 divisions provide accurate and timely intelligence, pertaining to indications and warnings, crisis developments, current operations, and conflict resolution.* [131]

A contemporary more comprehensive definition by the author would define and summarize the various intelligence activities and characters the following way:

Intelligence *is basically the combination of activities by government or private institutions with the purpose to win insights into the (a) behavior or planning of foreign states and of non-state institutions, (b) of economic activities, (c) of individuals or groups which includes hostile structures abroad or inside of friendly states, (d) using all ways and methods to win such information by using human, signal, technical and other means, and (e) can be structured in a number of ways like basic and enhanced intelligence, country reports, technical reports etc.*

The collection of information will use open or clandestine methods, like signal interpretation, defined as HUMINT, TECHINT, OSINT.

Intelligence organizations often specialize in offensive-, covert-, open-source-, or offensive & defensive intelligence operation departments, in counterintelligence, counter-terrorism, and early warning.

Generally, intelligence is either of political, military, strategic, operational, and tactical or of technical/technological or economic nature. Non-military intelligence is mainly economic-, technical- counter-terrorism- or organized crime-intelligence. Governments also will use methods of deception, subversion, agitation, and strategic communication and public diplomacy.

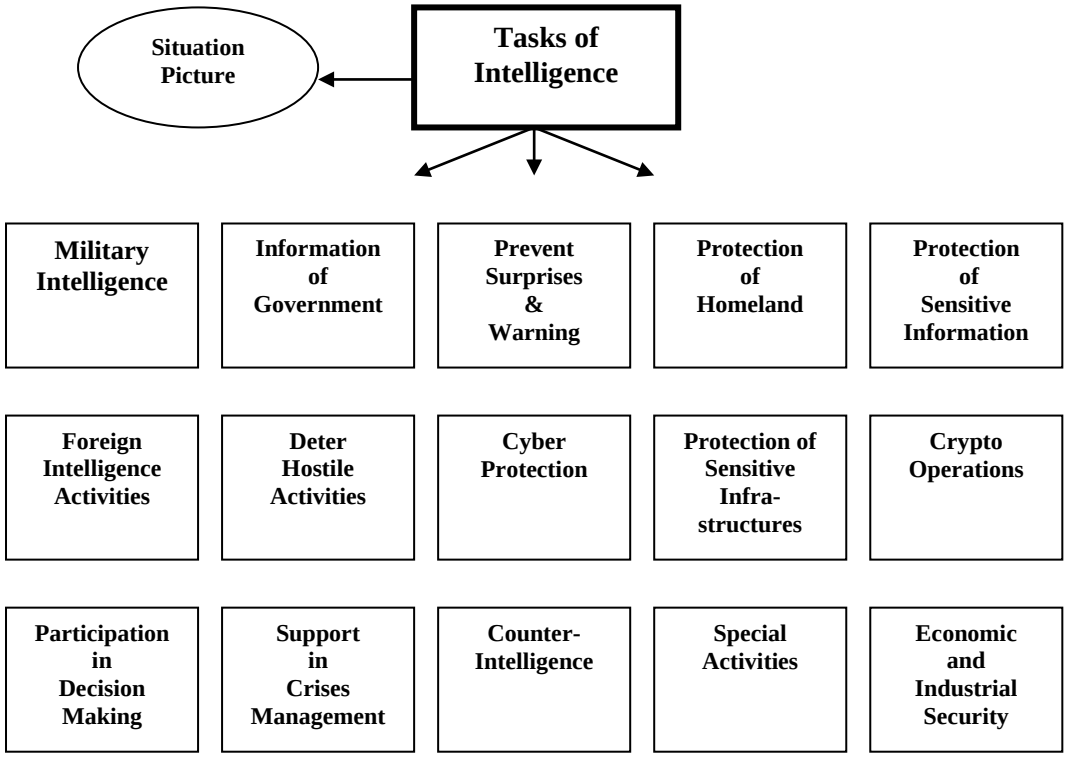
Intelligence can also be won by signal-interception, satellites, ground and aerial reconnaissance, by means of electronic (Net-Centric-) warfare etc. The information on hand will be collected, processed, analysed and disseminated in such a way that it can be provided for the user in the shortest possible way, whenever possible in real time."

Analysis of Intelligence

The organized information-base is processed by using deductive inference-techniques that integrates all data on hand in an attempt to answer the requester's needs.

Application of Intelligence

The intelligence product is disseminated to the user, providing answers to queries and estimates of accuracy of the product delivered. Products range from strategic intelligence estimates in the form of large hardcopy or softcopy (electronic) documents for policy makers, to real-time displays that visualize battlespace conditions for a war fighter.



Armed Forces Intelligence

Intelligence which integrates all military intelligence (ground, sea air, space, doctrine, politics, economy, science, society and other data, structured into strategic, tactical, order of battle, equipment, logistics, training, organization and manpower information of foreign nations. [132]

Basis Intelligence

It is knowledge on any subject that may be used as reference for planning and as basis for processing subsequent information or intelligence on a subject that is normally maintained in databases and is regularly updated. The main use of basis intelligence is to set the scene at the outset of operations. (AJP-2)

Basic Types of Intelligence

Intelligence is grouped into these basic categories:

- *Intelligence Estimate*
- *Monitoring, Assessment & Prediction*
- *Indications & Warning*
- *Basic Intelligence*
- *Current Intelligence*
- *Order of Battle Maintenance*
- *Support to other Warfare Areas*
- *Target Intelligence* (AJP-2)

Biographic Intelligence

The study of potential individuals of foreign nations, including their education and occupational history, status, attitudes, interests, habits and lifestyles. [133]

Collection

Following the plan, human and technical sources of data are tasked to perform the collection. The collection sources include both open and closed access sources and human and technical means of acquisition.

Collection Planning

Government and military decision makers define usually on a high level of information abstraction, the knowledge that is required to make policy, strategy, or operational decisions.

Combat Surveillance

A continuous, all-weather, day-and-night, systematic watch over the battle area to provide timely information for tactical combat operations. (AEDP-2, p. 20)

Communications Intelligence

Technical and intelligence information derived from foreign communications by other than the intended recipients. (AEDP-2, p. 20)

Counterintelligence

Information gathered and activities conducted to protect against: Espionage, other intelligence activities; sabotage or assassinations for or on behalf of foreign powers, organizations or individuals, terrorist activities; the physical protection of infrastructures; communication security; document security.

Counterintelligence includes active detection, penetration, identification and neutralization of individuals; the supervision of security programs; the collection, retention, processing, analysis and dissemination of evidence; combating hostile espionage; clandestine intelligence activities; the prevention of sabotage or planned assassinations.

Counterintelligence also includes the protection and analysis of hostile electronic (Cyber Warfare) activities.

Current Intelligence

a) *It reflects the current situation and is produced in response to intelligence requirements linked to a current operation and which refers to events at the time of the Operation.* (AJP-2)

b) Day to day events are presented with background and warning of near-term consequences.

Cyber Warfare

Cyber Warfare is the comprehensive approach to all electronic means of defensive and offensive methods to protect friendly and attack hostile electronic activities including, radio, data link, radar, relay, satellite, computer and other systems on the ground, in the air space and on sea.

Data (Types of)

Individual observations, measurements, and messages from the lowest to the most complex levels. It includes human communication, text messages, electronic queries, or scientific instruments that sense phenomena are the major sources of data. Data might be subject of various levels of protection.

Economic Intelligence

Economic analysis of foreign nations about the strengths and weaknesses of foreign nations, including capabilities, manufacturing, trade, economic warfare and economic vulnerabilities. [134]

Electronics Intelligence

Technical and intelligence information derived from foreign communications and electromagnetic radiation emanating from other than nuclear detonations or radioactive sources. (AEDP-2, p. 31)

Electronic Warfare

Military action involving the use of electromagnetic energy to determine, exploit, reduce or prevent hostile use of the electromagnetic spectrum and action which retains friendly use of the electromagnetic spectrum. (AEPD-2, p. 31) [135]

Estimative Intelligence

Assumptions of developments about possible outcomes beyond available facts.

HUMINT

All intelligence collected by individuals ("human sources) with or without technical means. HUMINT intelligence can be an open process, is hidden or uses clandestine methods. HUMINT includes data collection by diplomats, military attaches, media analysing, is mainly OSINT, but can include clandestine activities also. [136]

Imagery Intelligence

Intelligence information derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic devices, or other media. (AEDP-2, p. 45)

Influence Operations

Influence Operations should guide PSYOP and propaganda to affect the behavior of the population, especially to enhance operation security (OPSEC). They include psychological operations, military deception, counterpropaganda, strategic communication, Public Diplomacy and public affairs. [137]

Information

Organized sets of data are referred to as information. The organizational process may include sorting, classifying, or indexing and linking data to place data elements in relational context for subsequent searching and analysis. [138]

Information Security

Information security is paramount in societies, which depend on knowledge and information. The security of networks against cyber crime and cyber terrorism, sabotage, and espionage, is a national task. [139]

Intelligence

a) Information in the form of intelligence permits the forecast of possible future outcomes. Intelligence is usually the information and knowledge about an adversary obtained trough observation, investigation, analysis, or understanding. It is the product that provides battlespace awareness. Three major categories of military intelligence products can be distinguished: Strategic, Military-Operational, Military-Tactical.

b) *The product resulting from the collection, processing, integration, analysis, evaluation and interpretation of available information concerning foreign countries or areas.* (AAP-6)

c) *The product resulting from processing of information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations.*

d) The term is also applied to the activity, which results in the product, and to the organization engaged in such activity. (AAP-6, 2002)

Intelligence Cycle

The sequence of activities whereby information is obtained, assembled, converted into intelligence and made available to users. (AAP-6)

This sequence comprises the following four phases:

Direction:

> *Determination of intelligence requirements, planning the collection effort, issuance of orders and requests to collection agencies and maintenance of a continuous check of the productivity of such agencies.*

Collection:

> *The exploitation of sources by collection agencies and the delivery of the information obtained to the appropriate processing unit for the use in the production of intelligence.*

Processing:

> *The conversation of information into intelligence through collation, evaluation, analysis, integration and interpretation.*

Dissemination:

> *The timely conveyance of intelligence, in an appropriate form and by any suitable means, to those who need it.*

Intelligence Estimate

It should provide an analysis of a potential adversary's situation and assess his capabilities, intentions and probable courses of action.

Intelligence Mission

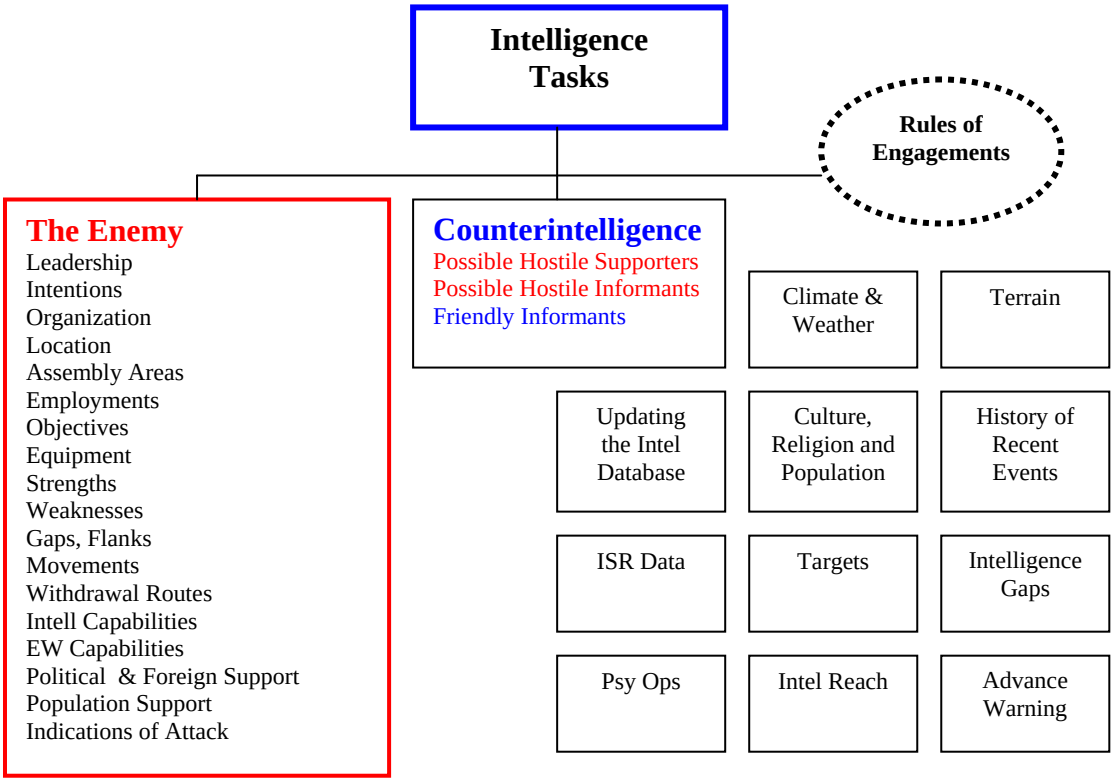
The intelligence mission is to provide intelligence, counter –intelligence, and security support to commanders and designated organizations and forces in peace, crisis and conflict. (AJP-2)

Intelligence Production

Intelligence may be produced in the format of dynamic visualizations in formal reports to policymakers. The categories of formal strategic and tactical intelligence reports are distinguished: (1) Current intelligence reports are news-like reports that describe recent events or indications and warnings; (2) basic intelligence reports provide complete descriptions of a specific situation; (3) intelligence estimates attempt to predict feasible future outcomes as a result of current situations, constraints, and the possible influences.

Intentions Analysis

Analysts have often the intention to follow in their judgments the "estimate of the consumers", which produced intelligence reports that politics wants to see. After such a conclusion becomes "official politics", it is nearly impossible to implement evidence, which would contradict such a policy.



Levels of Intelligence

The distinction between strategic, operational, and tactical intelligence is neither always clear, nor remains such intelligence over time in such specific brackets. Any information in one place can be purely tactical, but in another place or in connection to events will have a strategic dimension. The levels of intelligence is linked to the (current) levels seen by politics and military leadership either as *policy*, *strategic operations*, *tactical operations* and/or on a pure *tactical* level.

Knowledge

Information, once analyzed and understood, is "knowledge". Any understanding of information provides a certain degree of comprehension of both, the static and dynamic relationships of the objectives of data, and the ability to model structure and past content and dynamic process into current events to obtain a specific "picture".

In the military context, this level of understanding is referred to as "intelligence".

MASINT

MASINT is divided into radar, radiation, acoustic, laser, seismic, radio-frequency, electro-optical, nuclear, geophysical, biological and chemical intelligence.

Medical Intelligence

The collection of foreign medical and related information and health data to assess foreign medical capabilities. (MEDINT). The Department of Defense /DIA assesses such data in the Armed Forces Medical Intelligence Center.

Military Geographic Intelligence

Military intelligence about the geographic factors, features and demographics that may affect military operations. [140]

National Estimates

A *National Estimate* is an up-to date collection of important information of a foreign state, usually printed as a handbook, is SECRET or TOP SECRET, and includes all available information based on all available knowledge and intelligence. Some estimates are comprehensive, some deal with the political, economic or military development. Military data will include leadership and budget, will be structured along army, navy and air force, will give detailed information on organization, dislocation of forces, equipment, training, and relevant technical data. (See e.g. the CIA *Country Reports* from open sources.)

Operational Intelligence

It is the intelligence required in the planning, executing and supporting campaigns and operations by joint headquarters.

***Order of Battle Maintenance* (ORBAT)**

ORBAT contains traditional military data (maritime, ground, air, space, logistic etc.) and non-military data (proliferation, terrorism, environment etc.) reflecting the wider spectrum of NATO intelligence requirements. This data must be available as Basis Intelligence and/or Current Intelligence data.

The NATO Nations contribute to this agreed data published by the IMS Intelligence Division. Current intelligence will be maintained by NATO Headquarters/CJTF Headquarters using national intelligence contributions or intelligence collected by forces in or close to the Joint Operations Area. (AJP-2).

OSINT

Open Source intelligence is the collection of data, which are available from sources like books magazines, newspapers and news, meetings, Internet, radio and TV etc. Because of information provided by the many sources available.

(The former quite risky collection of information was replaced in the last years by an abundance of data found e.g. in the Internet.)

Political Intelligence

Collection of all political aspects of a foreign nation, including the structures of government, policies, political parties, propaganda and other political programs. [141]

Processing

The collected data is indexed and organized in an information base file, and is processed/monitored to meet the requirements of the collection plan or as requested by the command or authority.

Propaganda

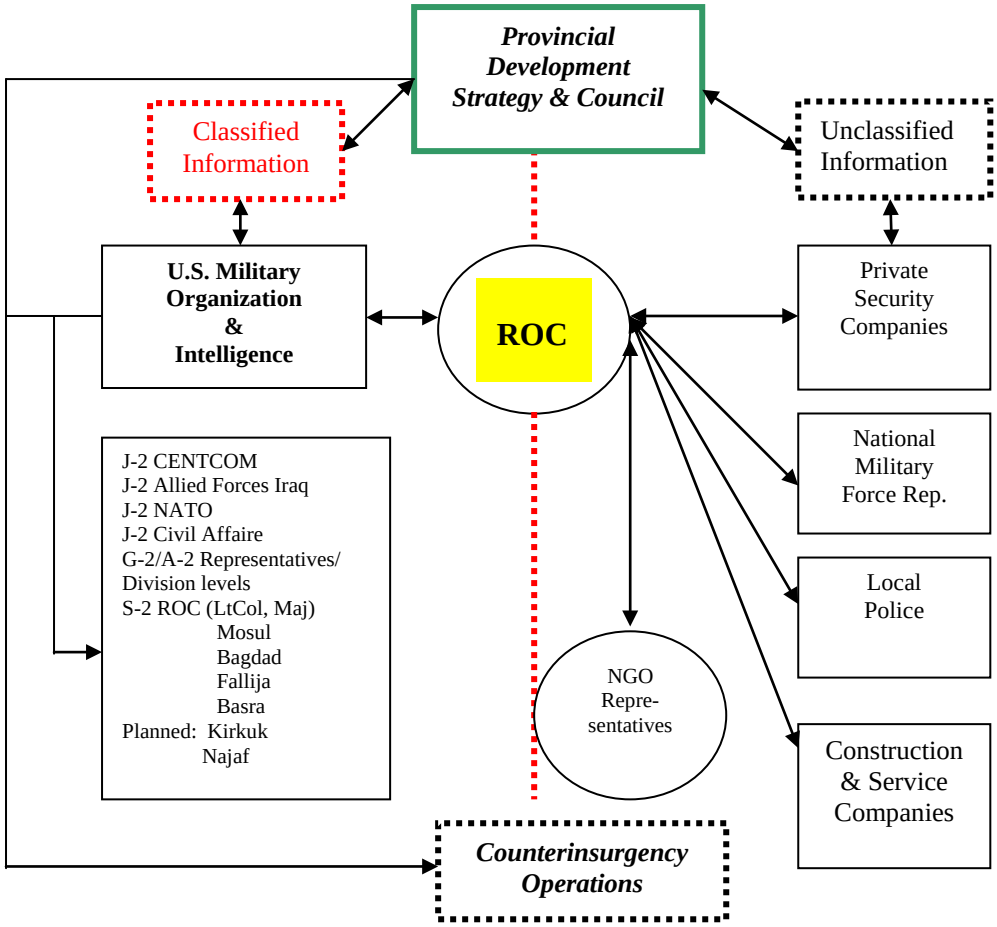
Propaganda is communication in support of national objectives with the purpose to influence opinions and attitudes of individuals in order to weaken the support of their government or regime, either directly or indirectly.

Provincial Reconstruction Teams

PRT were established for the first time in Iraq 2005, and at the end of 2007 there were 28 in place, 2008 the first were implemented in Afghanistan.

Nation Building/Societal Building regionally/locally implemented teams which work in a combined structure, including local authority, construction management, US-, UN-, NATO- and NGO-structures who are usually protected by friendly forces.

Intelligence is collected and provided. To maintain security the two sides of PRTs are usually separated.



Organization of a *Reconstruction Operation Center* (ROC) as established in Iraq in 2006-2009 and in Afghanistan in 2008. The red dotted line separates US/NATO/ISAF staff section from the non-military side.

Public Diplomacy

Presentation of political programs and explaining ongoing policy to the general public.

Reconnaissance

a) All technical means which help to find most recent developments or activities of military forces or opposing elements in a specific region. Reconnaissance is mainly based on ground, aerial, naval or space units or platforms and uses the eye, voice, film, optronics, IR, signal intercepts, and other sensors. Large area reconnaissance is the task of aircraft, UAVs, satellites, surface ships and submarines, reconnaissance units, Special Forces and so on.

b) A mission undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or potential enemy; or to secure data concerning the meteorological, hydrographic characteristics of a particular area. (AAP-6).

Science and Technological Intelligence [142]

Information on new developments, which might have an impact on national security, national scientific developments, or weapon systems capabilities. It would include a country`s overall

capabilities, armament, missile and space programs, nuclear energy and weapons, research, development and technology and other relevant sciences.

Secrecy

Secrecy is absolutely imperative to protect individuals, documents, planning, operations, and intelligence activities, to protect allies, troops in the field, in the air and on sea.[143]

Significant Activity (SIGACT)

Latest intelligence reported by battalion on the brigade S-2 levels and made immediately available to units operation in the field.[144]

SIGINT

Signals intelligence includes the intercept of information distributed by wire or telephone, encrypted and non-encrypted, and includes Communications Intelligence (COMINT) and Telemetry Intelligence (TELINT).

Situation Monitoring

Monitoring of a nation, region, military and non-military areas and activities, such as economic, ethnic and sociological factors, political developments and personalities involved in a nation`s leadership.

Sociological Intelligence [145]

It includes the population and demographic data, values, customs, morals, institutions, manpower, welfare, services, workforce, health and education, mass media and politics.

Sources

Intelligence sources are persons, conversations (HUMINT), pictures, maps, UAVs, and data collected by means of OSINT, SIGINT, IMINT, TECHINT, MASINT and Counter-Intelligence (CI).

Strategic Intelligence

This is the highest level of intelligence derived from information gathered over the widest possible area, in response to the requirements placed by national governments across the complete spectrum of national and international military, diplomatic, political and economic matters. (AJP-2)

STRATINT (Strategic Intelligence)

The collection of information, which has a strategic impact on the judgement regarding a foreign state, and would include all aspects of intelligence within such a scope. STRATINT is required for formulating policy and strategies. Most data will come from OSINT.

STATINT will also include *Strategic Warning*.

Strategic Intelligence Planning

The planning about intelligence gathering, priorities, requirements, organizations, personnel, budget, political oversight and regulations.

Support of other Warfare Areas

Intelligence will support a variety of other warfare areas such as electronic warfare and Information Operations (INFO OPS).

Surveillance

Surveillance is the real time-observation of specific areas, objects, infrastructures or persons of interests. The means of surveillance are aircraft, UAVs, radar, vehicles and agents, using all means of observation, including binoculars, cameras or IR-sensors, electronic and communication systems. Targets of surveillance are persons, ground, airspace, space and waters.

Tactical Intelligence

a) Intelligence of military and non-military character, which would support tactical planning and operations. Tactical intelligence in mainly the collection of battlefield relevant data, is mainly HUMINT respectively OSINT, SIGINT and TECHINT. It is collected, processes, and used on the levels of company, battalion, brigade and division, is processes by S-2, A-2 or J-2 levels, also for tactical-level combined and joint staffs.

b) *Is the intelligence required by tactical commanders for the planning and conduct of operations, from the level of formations headquarters downwards and produced within the formation's area.* (AJP-2)

Tactical Reconnaissance (TACRECCE)

Tactical reconnaissance is usually collected by ground forces in the field, by all kinds of ships (also civilian), or is flown by manned platforms and provides film or transmits real-time data to ground stations or other users and UAVs with sensors.

Target Intelligence

Finding, assessing and monitoring of targets, their positions, characteristics and other factors related to such targets and how to strike the targets.

TECHINT

TECHINT may include the collection of technical intelligence, but often is seen as a general term including also SIGINT (Signal Intelligence) which itself is often separated into COMINT (Communication Intelligence), RADINT (Radar Intelligence), IMINT (Imagery Intelligence, which includes electronically collected imagery, film, photographs, radar and infrared sensors, and electro-optic sensors), MASINT (Measurement and Signal/Signature Intelligence which is often used in a synonym way for RADINT, which includes radio, radar, nuclear, optical and other signature collection), ACOUSTINT (acoustic Intelligence), NUCINT (Nuclear Intelligence), LASINT (Laser Intelligence), IRINT (Infrared Intelligence), RINT (Radiation Intelligence), DEWINT (Direct weapons Intelligence) and GEOINT (Geospatial Intelligence). In a number of doctrines these different intelligence sources are listed separately and independently from TECHINT.

Transformation of Intelligence

Transformation included orientation, organization, communication, and cooperation, synchronizing of activities, new priorities.

Transportation and Telecommunication Intelligence [146]

Such intelligence studies transportation and communication means for military needs, but also during military emergencies and relief operations.

Warning Analysis

Warning analysis is either based on early signal-assessment or on ongoing political and military developments and is fed into situation pictures. Sherman Kent saw on the side of the "warners" the fear of "over waning", which he considered as dangerous for national security.

"Under warning" was seen as a defensive reaction against negative political reaction if warnings were wrong. Warning on the strategic level will include political, societal, military, economic, technological threat, nuclear threat, and terror warning.

Warning Intelligence

It presents developments on strategic levels, which might have consequences for the *National Interest*, foreign policy, defense and allies. Warning Intelligence should propose possible alternatives how to handle such developments.

Warning Process (Indications and Warning)

The warning process includes the interception of early signals pointing to certain developments at an early stage and will led through a complex process until facts will acknowledge early findings or prove their invalidity.

The warning process must be quick to be able to detect a change or changes in a wide spectrum of indicators. Changes may be interpreted as indicators that a nation or a region in which they are taking place is changing its political or military objectives and is preparing to adopt an altered political/strategic/defense posture, which may pose a risk to regional stability.

Abbreviations

A-2	Air Intelligence section in air or joint staffs
ACCS	Air Command Control System
ACLANT	Allied Command Atlantic
ACE	Allied Command Europe
ACO	Airborne Command Operations
ACT	Allied Command Transformation
ADAMS	Airborne Data Acquisition and Management System
AEDP	Allied Engineering Documentation Publication
AEI	American Enterprise Institute
AFDD	Air Force Doctrine Document
AFRICOM	U.S. Africa Command
AI	Artificial Intelligence
AID	U.S Department of State, Agency for International Development
AIFS	American Institute for Foreign studies
AJP	Allied Joint Publication
AMPS	Advances Mobile Phone System
ANSER	Department of Defense Think Tank
AOC	Allied Operations Command
AOCC	Air Operations Coordination Center
AP	Allied Publication
ASAS	All Source Analysis System
ATO	Air Tasking Order
ATOMAC	Atomic Materiel Containing (intelligence classification)
ATOMAL	Atomic Material
ATP	Allied Technical Publication
AWACS	Airborne Warning and Control System
AWG	Airborne Weapon Group
BATFE	Bureau of Alcohol, Tobacco, Firearms and Explosives
BCT	Brigade Combat Team
BICES	Battlefield Information and Collection Exploitation System
BIR	U.S Department of State, Bureau of Intelligence and Research
BMEWS	Ballistic Missile Early Warning System
BVR	Beyond Visual Range
C2	Command and Control
C3A	NATO Section
C3B	NATO Section

C4ISR	Command, Control, Communication, Computer, Intelligence, Surveillance and Reconnaissance
C4ISTAR	Command, Control, Communication, Computer, Intelligence, Surveillance, Target Acquisition and Reconnaissance
CAOC	Combined Air Operations Center
CC	Combined Command
CCIR	Commander's Critical Information Requirement
CCIRM	Collection Coordination Intelligence Requirements Management
CENTCOM	U.S. Central Command
CENTRIXT	Central Intelligence Exchange Network
CFTC	Commodity Futures Trading Commission
CFR	Council on Foreign Relations
CIA	Central Intelligence Agency
CIFA	Counter-Intelligence Field Activities
CHOTS	British forces secure communication system
CIMIC	Civil-Military Country Teams & Cooperation
COIN	Counterinsurgency
CPD&D	Collecting, Processing, Dissemination and Decisionmaking
CRC	(Air) Control and Reporting Center
CRS	Congressional Research Servcie
CSAR	Combat Search and Rescue
CSI	Center for the Study of Intelligence
CSIS	Center for Strategic and International Studies
CTS	Cosmic Top Secret
CYBERCOM	US Cyber Command
DARPA	Defense Advanced Research Projects Agency
DARS	Deployed Allied Reconnaissance Systems
DCAOC	Deployable Combined Air Operations Center
DEA	Drug Enforcement Agency
DIA	Defence Intelligence Agency
DNI	Director of National Intelligence
DoD	Department of Defense
DSS	Defense Security Service
ECM	Electronic Counter Measures
ELINT	Electronic Intelligence
EO	Executive Order
ESS	European Security Strategy
EUCOM	European Command
EUROPOL	European Police
EW	Early Warning

FBI	Federal Bureau of Information
FCC	Federal Communications Commission
FEMA	Federal Emergency Management Agency
FISA	Foreign Intelligence Surveillance Act
FM	Field Manual
FORCECOM	U.S. Forces Command
FPRI	Foreign Policy Research Institute
G-2	Military Intelligence Section in ground forces staffs
GPS	Global Positioning System
HS	Homeland Security
HR	House of Representatives Resolution
HUMINT	Human Intelligence
IB	Intelligence Board
ID	Intelligence Division
IDNX	Intelligence Data Network
IED	Improvised Explosive Devices
IFPA	Institute for Foreign Policy Analysis
ILU	Intelligence Liaison Unit
IMS	International Military Staff
INTERPOL	International (Criminal) Police Organization
IRTA	Intelligence Reform and Terrorism Act
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAF	International Security Assistance Force Afghanistan
ISR	Intelligence, Surveillance and Reconnaissance
ISR	Image Storage Retrieval
ISTAR	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IVSN	NATO Initial Voice Switch Network
J-1	Personnel Section in joint staffs
J-2	Intelligence Section in joint staffs
J-9	Concept Section in joint Staffs (experimentation, force integration, combat capabilities enhancement, leadership)
JAC	Joint Analysis Center
JCofS	Joint Chiefs of Staff
JCOP	Joint Common Operational Picture
JFC	Joint Forces Command
JSTAR	Joint Surveillance and Target Attack Radar System
JTIDS	Joint Tactical Information and Intelligence Distribution System

LOCE	Linked Operational Intelligence Centers in Europe
MAJIIC	Multisensor Aerospace –Ground Interoperable ISR Coalition Network
MC	Military Committee (NATO)
MCCIS	Military Command Control and Information Systems
MEADS	Medium Extended Air Defense System
MIDS	Multifunction Information Distribution System
MILTECH	Military Technology Intelligence
MITRE	Department of Defense Think Tank
MON	Memorandum of Notification
NADGE	NATO Air Defence Ground Environment
NAICS	NATO Armament Intelligence Coordination System
NATO	North Atlantic Treaty Organization
NAVAID	Navigational Aid
NC3A	NATO's Consultation, Command and Control Agency
NCC	National Communication Center
NCIX	National Counterintelligence Executive
NCTC	National Counter-Terrorism Center
NFFI	NATO Friendly Force Interface
NFIB	NATO Forces Intelligence Background (security classification)
NGIA	National Geospatial Intelligence Agency
NGO	Non-Governmental Organization
NIA	National Intelligence Agency
NIC	National Intelligence Council
NIDTS	NATO Intelligence Data Transmission Systems
NIE	National Intelligence Estimate
NIIA	NATO ISR Interoperability Architecture
NITF	National Imagery Transmission Format
NIWS	National Intelligence Warning System
NKWD	Soviet Security Intelligence (followed by the KGB)
NMD	National Missile Defense (Agency)
NOCONTACT	Intelligence security classification
NOFORN	Not to be distributed to Foreigners (intelligence security classification)
NORAD	North American Aerospace Defence Command
NRO	National Reconnaissance Office
NSA	National Security Agency
NSC	National Security Council
NSDD	National Security Directive Decision
OMB	Office of Management and Budget

ONE	Office of National Estimates
OODA	Observe, Orient, Decide and Act
ORCON	Use only with consent of the coordinating agency, security classification
OSINT	Open Source(s) Intelligence
OSS	Office of Strategic Services
PAIS	NATO Public Affairs International information System
PAP-T	Partnership Action Plan Against Terrorism
PDD	Presidential Decision Directive
PF	Presidential Findings
PfP	Partnership for Peace
PIR	Commander's Priority Intelligence Requirement
PROPIN	Proprietary Information involved
RAF	Royal Air Force (UK)
RAND	U.S. Think Tank
RASER	Rapid Analytical Support and Expeditionary Response
RCS	Radar Cross Section
REF	Rapid Equipping Force
RI	Request for Information
RL	Congressional Research Service Publication Code
RMA	Revolution of Military Affairs
ROE	Rules of Engagement
SACEUR	Supreme Allied Commander Europe
SACLANT	Supreme Allied Commander Atlantic
SAR	Synthetic Aperture Radar
SCIF	Sensitive Compartmented Information Facilities
SEC	Securities Exchange Commission
SEWWG	Signals Intelligence & Warfare Working Group
SHAPE	Supreme Headquarters Allied Powers Europe
SIGACT	Significant Intelligence
SIGINT	Signals Intelligence
SLBM	Submarine-Launched Ballistic Missile
SOC	(Air) Sector Operations Center
SOCOM	U.S. Special Operations Command
SOUTHCOM	U.S. Southern Command
SRI	SRI International (the former Stanford Research Institute)
STANAG	Standardization Agreement
STRATCOM	U.S. Strategic Command

TACRECCE	Tactical Reconnaissance
TARE	Telecommunication Automatic Relay Equipment
TECHINT	Technical Intelligence
THAAD	Terminal High Altitude Area Defense
TSA	Transportation Security Agency
TTIU	Terrorist Threat Intelligence Unit
UAV	Unmanned Aerial Vehicle
UKADGE	United Kingdom Air Defence Ground Environment
UMBRA	Top Secret document classification used by the CIA und NSA, including Stop Secret Dinar, Sabre, Spoke and Daunt
UN	United Nations
UPI	United Press International
USAF	U.S. Air Force
USC	U.S. legal code
USIA	United States Information Agency
USIB	U.S. Intelligence Board
USJFCOM	U.S. Joint Forces Command
USMC	U.S. Marine Corps
USMS	U.S. Maritime Service
USSS	U.S. Secret Service
USTRATCOM	U.S. Strategic Command
WMD	Weapons of Mass Destruction

Notes

Comments on the Notes: The listed sources resemble only a small amount of literature dealing with intelligence matters and problems.

---

1 MC 64/9 NATO Electronic Warfare (EW) Policy; MC 133/3 NATO Operational Planning System; MC 161 NATO Strategic Intelligence Estimate (NSIE); MC 362/1 NATO Rules of Engagement; MC 402/1 NATO Policy of Psychological Operations; MC 411/1 NATO Civil-Military Co-operation Policy; MC 422/1 Information Operations Policy; MC 457 NATO Military Policy on Public Information; MC 472 NATO Military Concept for Defense against Terrorism; C-M (2002) 49 Security within NATO; NATO Crisis Response System Manual (NCRSM); AJP-01 Allied Joint Doctrine; AJP-3 (A) Allied Joint Operations; AJP-3.6 Allied Joint Electronic Warfare Doctrine; AJP 3.10 Allied Joint Doctrine for Information Operations, AJP-5 Allied Joint Doctrine for Operational Planning etc.

2 The fact is, that even in the Second World War intelligence sharing between allies was quite limited.

3 Wesley K. Clark: Winning Modern Wars. Iraq, Terrorism, and the American Empire. Public Affairs/Perseus Books Group, Cambridge, MA, 2003; Rupert Smith: The Utility of Force. The Art of War in the Modern World. Allen Lane, London, 2005 etc.

4 Grace V. Jean: 'Culture Maps` Becoming Essential Tools of War, National Defense Magazine, Feb. 2010, http://www.nationaldefensemagazine.org/archive/2010/February.

5 This works on a "give and take"- basis. Because currently the number of PfP-states is dwindling, it can be assumed that the overlapping of nationally collected intelligence data covers more and more details of other states. In the Balkans such intelligence made e.g. Austria's intelligence input redundant.

6 Rowan Scarborough: Exclusive: Lack of translators hurts U.S. war on terror, Report, Aug 31, 2009. FBI, DIA, NSA and CIA are channeling urgent intercepts in Arabic, Pashto, Dari, Urdu, Kurdish to language offices and translation centers. But there are shortages also in Chinese, Russian etc.

7 The option of a possible Iwo Jima landing emerged at the end of 1943, and intelligence data was updated until the landing on Feb 19, 1945, mainly based on 200 photo reconnaissance mission flown by aircraft. The final intelligence estimate made by the Joint Intelligence Center, Pacific Ocean Areas, Pearl Harbor, expected 13.500 Japanese soldiers on the island (there were 23.000), counted 234 guns of all kinds (there were 361), also, the Japanese would defend the beaches like on Guam, Tinian, Peleliu because of built trenches (but they did not), most defensive positions and resistance would be encountered in the south (they were encountered in the north). Because of intelligence, US naval bombardment was partially concentrated on wrong targets and heavy casualties.

8 John Bolton: Let`s Take Bureaucracy Out of Intelligence, The Wall Street Journal, Jan. 10, 2010. Online wsj article.

9 Michael Crowley: Intelligence Design, The New Republic, Feb. 4, 2009.

10 FM 2-0, Intelligence, Headquarters Department of the Army, Washington, DC, 23 March, 2010.

11 U.S. Army FM 2-01.3, U.S. Marine Corps MCRP 2-3A Intelligence Preparation of the Battlefield/Battlespace, U.S. Army Intelligence Center, Fort Huachuca, AT, Oct 2009.

12 Dale Meyerrose, Associate Director of National Intelligence and Chief Information Officer/Intelligence Community Information Sharing Executive.

13 Published by the Director of National Intelligence, J. M. McConnell, Feb. 2008. Sharing will follow the "Need to Know" but also includes the "Responsibility to Provide", will be "Enterprise Centric", "Mission Centric", "Information Centric", analysis will be multi-dimensional.

14 Dennis Blair, Director National Intelligence, August 2009.

15 John G. Heidenrich: The State of Strategic Intelligence. CSI, CIA Home Library, June 8, 2008, 24 pages; The Blueprint for the U.S. National Intelligence Strategy, Sept. 16, 2009. Director of National Intelligence Dennis C. Blair identified these aims of national security policy and strategic intelligence: Combat Violent Extremism; Counter WMD Proliferation; Provide Strategic Intelligence and Warning; Integrate Counterintelligence Capabilities; Enhance Cybersecurity; Support Current Operations.

16 Interview: Gen. Peter Chiarelli, U.S. Army Vice Chief of Staff, Defense News, April 20, 2009, p. 30.

17 Dag Wilhelmsen: We are looking to C4ISR to develop our operational and security environment, JDW, 25. Feb. 2009, p. 34. The work of NC3A includes a better Joint Common Operational Picture (JCOP) and recommends improved control of blue force-units (blue force tracking) with the new NATO Friendly Force Interface (NFFI). See: Kris Osborn; NATO Seeks To Link Members` Blue-Force Tracking, Defense News, Aug 4, 2008, p. 6.

18 See also FM 3.24 Counterinsurgency, and comments on further research projects. Many sources, see: Steven L. Bullimore: The Military's Role in Nation Building: Peace and Stability Operations Redefined. U.S. Army War College, Carlisle, PA, March 2006.

19 Kris Osborn: U.S. Army Taps Cultural Intelligence, Defense News, April 7, 2008, p. 42. However, cultural intelligence goes back to 1942, when the OSS used social sciences in OSS intelligence which included political science, economics, statistics, history, social psychology, sociology, anthropology, geography, moral of public, government, political institutions, social structures and institutions, ethics and customs, population, health and sanitation, natural resources, agriculture, finances, national aspirations, terrain and climate, transportation. Source: OSS Descriptive Intelligence, graphic, 1942, no further data.

20 Bill Sweetman, Tony Banks: Techint v. Humint: The unseen war. Jane's Defense Weekly, 16 Feb. 1991, p. 221.

21 Joint Special Operations, Joint Publication FM 3-05.1, Department of Defense, Washington, DC, 2007.

22 FM 3-24, Counterinsurgency, Department of the Army, Washington, DC, 2006. The way the FM 3.24 is implemented was described by the author in ÖMZ

23 Air Force Doctrine Document 2-3, Irregular Warfare, Department of the Air Force, Washington, DC, 2007.

24 See the creation of the NSA, DIA, NRO etc. Non-military intelligence and counterintelligence (CIA, FBI, USSS, BIR) was rarely changed. Richard A. Best: Proposals for Intelligence Reorganization, 1949-2004. CRS Report for Congress RL 32500, Congressional Research Service, The Library of Congress, Washington, DC, Sept. 2004.

25 Defensenews.com/story.php?F=3136344&C=Americas, Nov. 2, 2007.

26 There are 16 major intelligence agencies, but additionally there are other government organizations as well, dealing with terrorism, internal security, organized crime, industrial security, infrastructure protection, military (operational) intelligence, or provide intelligence data for Government, Congress, or provide specific advise: CIA, DIA, NSA, NRO, NGIA, NCTC, DSS, USSS, USMS, NIC, FCC, NCC, FBI (here mainly the National Security Division), Defense Information Systems Agency, BIR, DEA, USIAS, TSA, BATFE, Energy Department, US Army Intelligence and Security Command, Office of Naval Intelligence, Naval Oceanographic Office, U.S. Air Force Intelligence Surveillance and Reconnaissance Agency, USMC Intelligence, Coast Guard Intelligence, furthermore 12 J-2 staff departments (Joint Intelligence Center) of the Unified/Combatant Commands, plus the US Border Patrol. Additionally, there are other institutions like the Congressional Research Service, USIA, AID, the State Department's Bureau of Diplomatic Security, the Defense Department's CIFA and Defense Investigative Service, the Office of Nonproliferation and National Security, the Securities and Exchange Commission (SEC, investigating money laundering), the Commodity Futures Trading Commission (CFTC, merchandise issues, supervises sanctions policy), the Office of Intelligence Support of the Treasure Department, the Federal Emergency Management Agency (FEMA) and a number of medical institutions. Also assessing intelligence are: RAND, MITRE, ANSER, and other think tanks who provide reports and assessments like Heritage, Brookings, CFR, CSIS, Hudson, BDM, SRI International, FPRI, IFPA, Center for Naval Analyses, AEI, World Resources Institute, Carnegie Endowment for International Peace and many more.

27 The Intelligence Community in the 21st Century. The Intelligence Community Act of 1996, Findings, June 1996. U.S. House of Representatives, Permanent Select Committee on Intelligence, Washington, DC, June 1996. The very detailed report with a historical overview of U.S Intelligence since 1775, is listing all legislative acts, is describing the work of the intelligence community, but the findings recommended a total overhaul of the intelligence agencies, and proposed an overview of all foreign intelligence activities of the NSC, the DCI, the CIA, NSA, DIA and BIR. It also recommends a single head for military intelligence (recommended is the J-2/JCofS), and a technological- and clandestine-intelligence branch. NIEs should be free of policy preferences. Included are the hearing protocols of Carlucci, Nye, Inman and Haass.

28 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism*. (USA Patriot Act of 2001, Public Law 107-56, Oct. 26, 2001). Additionally, there is s number of

other laws, like the *Communications Act* (1934), the *Foreign Intelligence Surveillance Act* (FISA, 1978), the *Civil Service Reform Act* (1978), the *International Money Laundering Abatement and Anti-Terrorist Financing Act* (2001), the *Intelligence Reform and Terrorism Prevention Act* (IRTPA, 2004) etc.

29 See: The National Intelligence Strategy of the United States of America (Oct. 2005); Douglas F. Garthoff: Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946-2004. Washington, DC: Potomac Books, 2007.

30 Elizabeth B. Bazan: The Foreign Intelligence Surveillance Act: A Brief Overview of Selected Issues, CRS Report for Congress, RL 34279, Congressional Research Service, The Library of Congress, Washington, DC, 2007; U.S.C. § 1801, FISA. See: Elizabeth B. Bazan: Foreign Intelligence Surveillance Act: Selected Legislation from the 108th Congress. CRS Report for Congress, RL 32608, Congressional Research Service, The Library of Congress, Jan 11, 2005. See also: Myth/Fact: Key Myths About FISA Amendments in the Protect America Act. The White House, Office of the Press Secretary, Sept. 18, 2007.

31 The NIC was established with EO 12036 (1978), recommended by Adm. Stansfield Turner, and was reorganized with EO 12333. The NIC provided intelligence papers for the National Security Council, the Department of Defense, and State Department.

32 The Estimates were standardized in 1950, when CIA Director LtGen Walter Beddel Smith created the Office of National Estimates (ONE), run by Sherman Kent, then with 12 country experts and 30 additional specialists. EO 12036 became also the guidance document for the production of future National Intelligence Estimates within the CIA. NIEs were also distributed to a number of allies.

33 Loch K. Johnson: Accountability and America's Secret Foreign Policy: Keeping a Legislative Eye on the Central Intelligence Agency. Foreign Policy Analysis, March 2005, pp. 99-120; Todd M. Masse: The National Counterterrorism Center: Implementation Challenges and Issues for Congress, CRS Report for Congress, RL32816, March 24, 2005.

34 Shaun Waterman: Analysis: More change to U.S. spy agencies, UPI, Aug.1, 2008. These changes were written into EO 13470, in fact a revision of EO 12333 of 1981, again amended (as EOs 13.284 and 13355, then by EO 13470) and was mainly affecting the authority of the DNI, which was given a stronger position within the intelligence community and the NSC.

35 Mike McConnell: Overhauling Intelligence, Foreign Affairs, July/August 2007, pp. 49-58.

36 Helen Fessenden: The Limits of Intelligence Reform, Foreign Affairs, Nov./Dec. 2005, pp. 106-120; Jeffrey Harris: Intel Restructuring, Defense News, Dec. 13, 2004, p. 29; Frederick M. Kaiser: A Joint Committee on Intelligence and Alternatives: Proposals from the 9/11 Commission and Others. CRS Report for Congress. RL 32525, Congressional Research Service, Dec. 20, 2006; Harold Kennedy: Intelligence Sharing; "Still a Battle", National Defense, June 2006; Inside Intelligence – Reforming the US Intelligence Community, International Security, Jane's Intelligence Review, Oct 1, 2007. There are many other articles coming to the same conclusions.

37 Paul Kane, Ben Pershing: Secret Program Fuels CIA-Congress Dispute, Washington Post, July 10, 2009, p. A1. (See also below.)

38 Many sources; see: Ed O`Keefe: Eye Opener: Intelligence Turf War. The Washington Post, June 28, 2009, p. A1.

39 LtGen David Deptula, Director Air Force intelligence, consolidated all reconnaissance and surveillance operations under his supervision, which also included Air Force TECHINT and SIGINT data, recce and surveillance equipment and UAVs. This immediately raised critical reactions from the Navy and Army and their specific program oversight and procurements. See: Caitlin Harrington: US Air Force debates control of IST assets, JDW, 11. April 2007, p. 8. See also: Remarks by the President on Intelligence Reform, Aug. 2, 2004, 5 pages.

40 See: Congressional Reports: H.R. 108-796 – Intelligence Reform and Terrorism Prevention Act of 2004. Superintendent of Documents, Government Printing Office, 2004.

41 Gordon Lederman: Making Intelligence Reform Work. American Interest, Spring 2009, pp. 23-31.

42 Richard Lardner (AP): US intelligence gathering in Afghanistan, July 23, 2009 (Yahoo News).

43 It will become fully operational in October 2010, headquarters will be at Ft. Meade, MD. In its offensive operations it will be mainly supported by the USAF (24th Air Force/Air Force Space Command), and in its "defensive" work by the NSA, which will act for the time being as a supervising agency.

[44] Based on the *Report of The Commission on Cyber Security for the 44th President*, December 2008.

[45] The registers for PFs and MONs are TOP SECRET and were never subject of the Freedom of Information Act.

[46] NSDD 159, January 18, 1985: *Covert Action Policy Approval and Coordination Procedures*. NSC, TOP SECRET/VEIL.

[47] Kristin Archick, Paul Gallis: NATO and the European Union, CRS Report for Congress, RL 32342, Congressional Research Service, Washington, DC, 2008; Nicholas Fiorenza: NATO, EU Defining Force Roles, Mission, Defense News, May 17, 2004; Stephen J. Flanagan: Sustaining U.S.-European Global Security Cooperation, Strategic Forum No. 217, National Defense University, Washington, DC, Sept. 2005; POP Adrian: NATO and the European Union. Cooperation and Security, NATO Document, Review 2007, Issue 2; Zachary Selden: Stabilization and Democratization: Renewing the Transatlantic Partnership, Parameters, Winter 2007/08, pp. 85-98; Brooks Tigner: Stronger NATO-EU Defense Ties Sought, Defense News, Oct. 20, 2003, p. 8; U.S.-EU Summit Declaration: Promoting Peace, Human Rights and Democracy Worldwide, The White House, George W. Bush, News Release, June 21, 2006, 12 pages, President Discusses American and European Alliance in Belgium, The White House, George W. Bush, Feb. 2005, 7 pages.

[48] Many sources, see e.g.: John Kriendler: NATO Intelligence and Early Warning. Conflict Studies Research Center, March 2006 (Special Series 06/13).

[49] Described in many papers, especially the ones criticizing the European Security Strategy (ESS) of 2003, the limited involvements in Africa, the non-involvement in Iraq, and declines by a number of states to raise troop levels in Afghanistan. For an overview see: Kristin Archik, Paul Gallis: NATO and the European Union, CRS Report for Congress, RL 32342, Washington, DC, Jan. 2008.

[50] NATO has on the strategic level two air commands (CC Air Ramstein, GE, CC Air Izmir, TR). The NADGE/ACCS includes on the operational level six combined/deployable air operation centers (CAOC, DCAOC, Udem (2), Finderup, Poggio Renatico (2), Larissa), national air defense wings, groups and squadrons (fighters, missile sites) are parts of the air defense organizations. Additionally, there are also a number of deployable radar systems available on national levels. See: Giles Ebutt: NATO`s integrated air command and control system advances to next stage, Jane's International Defense Review, Aug. 2007, pp. 53-57; Joris Janssen Lok: NATO deploys new air centre, JWD, 6 July, 2005, p. 5; Michael L. McGinnis: A Deployable Joint HQs for the NATO Response Force, Military Technology/MILTECH 4/2007, pp. 72-78.

[51] NATO owns and operates a number of communication systems or uses national networks like TARE, IVSN, MAXIMA, NIDTS, IDNX, PROMINA, CRONOS, AIFS/AMPS, MCCIS, PAIS, CRESP, ADAMS and Internet. See: Thomas Wirsching: NATO-Fernmelde und Informationssysteme, Soldat und Technik, 8/2000, pp. 493-498.

[52] The Fusion Center war proposed by Allied Command Transformation, and was originally seen as a coordination center of the war against terrorism within NATO. Bryan Mitchell: NATO Intelligence Fusion Center opens in England, Stars and Stripes, Oct. 17, 2006, p.1; Laurence Mixon: Requirements and Challenges Facing the NATO Intelligence Fusion Center. The Air War College, Air University, Maxwell AFB, 2007; New NATO Intelligence Center Opens in Britain, Defense News, 16 Oct. 2006.

[53] Currently, data is "actively" collected on approximately 80 states, on space, land, air and naval/marine forces and systems, technology, weapons, WMDs, hostile intelligence, medicine, communications, cyber networks and software, submarine warfare, public information, missile defense, satellite security, operational data, meteorology and climate, infrastructures, terrorism, provided by NATO member states, some from NATO PfP-states, from commands, the G-2/A-2 branches, the NATO Armaments Groups, NATO Economic Committee, NATO Air Defense Committee, NATO Science Committee, Defense Research and Technology, various security details, counter-terrorism etc. Data also comes from open sources like SIPRI, Military Technology, Jane`s books, Weyer`s, handbooks, magazines etc.

[54] Klaus Naumann, John Shalikashvili, The Lord Inge, Jacques Lanxade, Henk van den Breemen: Towards a Grand Strategy for an Uncertain World. Renewing Transatlantic Partnership. Lunteren: Noaber Foundation, 2007, p. 142.

[55] Colin Clark: Create Intelligence Interpol for U.S., Allies, Defense News, Aug. 9, 2004, p. 21; Scott Gourley: US explores allies` strategic right to know, JDW, June 15, 2005, p. 79; Laura M. Colarusso, Gail Kaufman, Gopal Ratman, Megan Scully: U.S. To Share Intelligence With More Allies, Defense News, Nov. 24, 2003, p. 12.

56 MC 362/1, NATO Rules of Engagement.

57 James L. Jones: A Blueprint for Change: Transforming NATO Special Operations, JFQ, 2/2007, pp. 36-40. U.S., NATO and EU forces operate HH-60G, HH-60H, MH-60K *Pave Hawk*, CH-53E, MH-53J, MH-53M *Pave Low*, HH-47, MH-47E and MH-47G *Chinook*, EC-725/EC 225/AS 352 *Cougar*, SA 330 *Puma*, EH-101 CSAR, HH-3F, and in the future the U.S. forces will operate HV- and MV-22. CSAR helicopters have special avionics, are partially armored (Kevlar), carry weapons, ECM equipment, additional fuel tanks, and special navigation and communications equipment. For an operational assessment see: James L. Jones: Transforming NATO Special Operations. A Blueprint for Change. JFQ, 2/2007, pp. 36-40.

58 Andrew Chuter: A New ISTAR Capability for U.K.? Defense News, June 9, 2008; Ivan Costica, Razvan Mofleanu: ISTAR System, Intelligence, Rumanian Military Thinking 1/2007, pp. 97-103; Tim Ripley: Taking the High Road, JDW, 1 March 2006, pp. 24-29; Richard Scott: UK studies ISTAR requirements, JDW, 31 March 2004, p. 14; Bill Sweetman: ISTAR platform battles loom in transition to new security era, Jane's international Defence Review, March 2006, pp. 46-49.

59 STANAG 2129, STANAG 4579.

60 Lolita C. Baldor: Computer attack may be linked to N. Korea, San Diego Union Tribune, July 9, 2009, p.1, Chris Lefkow: W. House, DoD Web Sites Targeted by Cyberattack, Defense News, 8 July, 2009. The attacks were aimed at the White House, Department of Defense, Federal Trade Commission, Voice of America, Department of Transportation, Federal Aviation Administration, Department of Homeland Security, NSA, State Department, U.S. Postal Service, U.S. Treasury Department etc.

61 Stanton Sloane: The role of ´cyber czar`, Armed Forces Journal, September 2009.

62 Mark Thompson: U.S. Cyberwar Strategy: The Pentagon Plans to Attack. TIME, Feb. 2, 2010, http://www.time.com/time/printout/nation/article.

63 There are more than 800 entries in the DoD Cyber War files and a dozen manuals, recommendations, studies about cyber war, some coming from private companies like the Northrop Study about China`s cyber war and cyber espionage against the U.S.

64 NATO C3 Agency, Operations Research Applications Development, with descriptions about the new systems: http://www.nc3a.nato.int/organization/ad.html.

65 Sebastian Sprenger: NATO Scrambling to Improve Intel Sharing, But Obstacles Remain. World Politics Review, Inside the Pentagon, 26 Oct 2006, http:://www.worldpoliticsreview.com/Article.aspx?id=296, 3 pages.

66 Intellipedia, implemented in April 2004, is a firewalled Intranet information system, which is structured like the Wikipedia, Google or Yahoo web-search archives. It is not available for intelligence agencies outside the U.S., and contains only intelligence- valuable data, including counterterrorism. Intelipedia had at the end of 2007 approx. 50.000 pages of information. The idea goes back to 2004, when the U.S. Air Force proposed a "Google"-like information sharing system, called then Distributed Common Ground System (DCGS) to distribute information in near-real time to user, connecting providers and users. This idea was immediately suggested for the whole intelligence community and supported by Donald Rumsfeld and John Negroponte. The software was provided by Wikipedia (Jimmy Wales) but was especially tailored to the needs of intelligence customers. The software came from a team gathered by Chris Rasmussen. See: Bill Ives, Creating Successful Niche Content Spaces on the Web: Lessons for Enterprise 2.0, http://www.fastforwardblog.com/2007/03/28; Glenn W. Goodman: Net-centric Trailblazer. Services Jointly Pursue ´Google`-like Info-Sharing System, Defense News, March 8, 2004, p. 22.

67 NATO`s eastern enlargement, and the NATO *Partnership for Peace*, was the idea of Joseph J. Kruzel and Strobe Talbott, supported by Madeleine Albright, originally aimed at Poland, Hungary and CSSR. It was implemented in 1993, but was originally not supported by the French which feared for the idea of an independent European Security and Defense Identity (ESDI) under the umbrella of the then European Community and the CSCE.

68 Ted Galen Carpenter: NATO enters the 21ste century. Routledge-Curzon, London, 2000; Heinz Brill: Die NATO-Osterweiterung und die geopolitischen Interessen der Mächte, ÖMZ 6/98, pp. 637-648; John Hillen, Michael P. Noonan: The Geopolitics of NATO Enlargement, Parameters, Autumn 1998, pp. 21-34; Sean Kay: NATO`s Open Door. Security Dialogue, Vol. 32, 2, pp. 201-215.

69 Michael D. Maples, LtGen, Director DIA: Current and Projected National Security Threats to the United States. Statement for the Record, Senate Armed Services Committee, 27 Feb. 2007.

[70] Sebastian Sprenger: NATO Scrambling to Improve Intel Sharing, But Obstacles Remain. World Politics Review, Inside the Pentagon, 26 Oct 2006, http:://www.worldpoliticsreview.com/Article.aspx?id=296.

[71] MC 161, NATO Strategic Intelligence Estimate (NSIE)

[72] Developments come mainly from the *Signals Intelligence & Electronic Warfare Working Group* (SEWWG).

[73] NATO area and the USEUCOM area are geographically different.

[74] In the early 1980s, the staff of the SACEUR was divided into the operational side of the staff with the G-2 and G-3, and the logistic side with the G-1 and G-4 branches. In the early 1990s the G-5, G-6 and G-7 were added to the "operational side", the G-8 and G-9 to the logistic side. Reorganization occurred in the mid-1990s, and one more in 1994, when the Gs were changed into Js, following the new U.S. staff structure. Not all lower-level staffs have all enumerated staff branches.

[75] LOCE is a US developed terminal-centered PC web-enabled information system for classified intelligence data and is connected to CRONOS (SHAPE) und BICES.

[76] CENTRIXT is connecting also ships, AWACS, the State Department and US embassies.

[77] See: NATO Open Source Intelligence Reader, February 2002; NATO Intelligence Exploitation of the Internet, SACLANT, Norfolk, VA, October 2002.

[78] James B. Ellsworth: Eyes on Target. Intelligence Support to an Effects-based Approach, JFQ 27, 3d quarter 2007, pp. 27-31.

[79] Siehe: MC 161 NATO Strategic Intelligence Estimate.

[80] The US Department of Commerce, Washington, DC, August 16, 2007, contracted CIRM software. The system description is based on the requirement of NAICS, CCIRM-TOOLS-SURVEY and had to be fully compatible and operational with existing hardware.

[81] Raymond T. Odierno, Nichoel E. Brooks, Francesco P. Mastracchino: ISR Evolution in the Iraqi Theater, JFQ No. 50, 3d Qu. 2008, pp. 51-55; Michael Flynn, Rich Juergens, Thomas L. Cantrell: Employing IST – SOF Best Practices, JFQ No. 50, 3d Qu. 2008, pp.556-61.

[82] See as outstanding examples for such estimates: Richard L. Kugler, Ellen L. Frost: The Global Century. Globalization and National Security. National Defense University, Fort Leslie McNair, Washington, DC, 2001; Mapping the Global Future. Report of the National Intelligence Council's 2020 Project, Government Printing Office, Washington, DC, 2004.

[83] Hans Binnendijk, David Gompert, Richard L. Kugler: A New Military Framework for NATO, National Defense University, Fort Leslie McNair, Washington, DC, 2005. See also the political problems between NATO and EU, which would have an effect on intelligence sharing as well: Bernard von Plate: Die Zukunft des transatlantischen Verhältnisses: Mehr als die NATO. SWP-Studie, S 17, Mai 2003, Berlin. For an overview see also: Gunther Hauser: Die NATO – Transformation, Aufgaben, Ziele. Frankfurt am Main: Peter Lang, 2008.

[84] Megan Scully: Out of touch. Policies, technology hindered data-sharing with allies in Iraq, IS&R Journal, May 2004, p. 32. See also p.6 with reports about lack of collaboration of the intelligence services.

[85] See: Human Intelligence Collector Operations, FM 2-22.3 (FM 34-52), Dept of the Army, 2006; Megan Scully: ´Social Intel` New Tool for U.S. Military. Intelligence Increasingly Focuses on Relationships Among Individuals, Defense News, April 26, 2004, p. 13.

[86] Nik Gowing: Real-Time Crises: New Real-Time Information Tensions. In: Faster and more united? The debate about Europe's crisis response capacity. European Commission, Brussels, 2007, pp. 275-278; Michaelis Koutouzis: Interpreting Time and Space, and Foreseeing Crises. In: Faster and more united? The debate about Europe's crisis response capacity. European Commission, Brussels, 2007, pp. 279-284.

[87] C-M (2002) 49 Security within NATO; C-N (2002) 50 Protection Measures for NATO Civil and Military Bodies of Deployed NATO Forces and Installations against Terrorist Threats; Allied Command Operations Force Protection Directive 80-25, 2006 - Functional Planning Guide, Force Protection.

[88] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[89] McCarran Act, with some long-term implications for the allies because it made membership of a communist party a subversive act and also changed the rules for immigration and travel to the U.S. The observation of U.S. citizens was the task of the FBI.

[90] The strategic level of NATO was SACLANT/ACLANT, but that was discontinued in 2004, and this level became Allied Command Transformation (ACT), which is not anymore a strategic "command" and does not have a command-staff structure. ACO/SHAPE is the military-strategic level and is on top of three Joint Forces Commands (JFC, Brunssum, Naples and Lisbon), which act as operational commands. On the component (tactical) command level are CC Heidelberg, CC Air Ramstein, CC Marine Northwood, CC Land Madrid, CC Air Izmir, and CC Marine Naples, and they are providing ground forces, naval forces, air forces (air defense and offensive forces) to the JFCs in Europe and for *out-of-area* operational areas. JFC Brunssum operationally controls currently the ISAF force in Afghanistan.

[91] See e.g. 4545, 4559. 4586, 4607, 4609, 7023, 7085…

[92] Command, Control, Communication and Computer, Intelligence, Surveillance and Reconnaissance.

[93] Command, Control, Communication and Computer, Intelligence, Surveillance, Target Acquisition and Reconnaissance, which is mainly an (strategic) air power/air operations network that includes policy, doctrine, concepts, Air C2, space and interoperability/air, airpower management; on the operational level AWACS, air-ground surveillance, airspace control, imagery dissemination, interoperability; on the tactical level platforms and UAVs, Data Link, NAVAIDS, meteorology, capability integration.

[94] Allied Engineering Documentation Publications for NATO Intelligence, Surveillance, and Reconnaissance Interoperability Architecture (NIIA).

[95] CRONOS is also compatible to the U.S. Secret Internet Router Network (SIPR-Net) and the British CHOTS and FIRECREST.

[96] Harold Kennedy: Intelligence Sharing; "Still a Battle", National Defense, June 2006.

[97] Andrew W. Green: It's Mine! Why the US Intelligence Community Does Not Share Information. School of Advanced Air and Space Studies, Maxwell AFB, AL, 2005; Many sources, see e.g.: John Kriendler: NATO Intelligence and Early Warning. Conflict Studies Research Center, March 2006 (Special Series 06/13).

[98] The "Need to Know" policy has its drawbacks: Often it is not known what is needed, it is not known what other staffs might need, and to them it is not known what information is available. (So Donald Rumsfeld)

[99] NATO experienced over the years a number of rather severe intelligence cases involving officers, civilian employees etc. A case, which was made public, involved the French major Pierre-Henri Bunel, who worked in NATO planning and supplied secret air-attack data of NATO in 1999 to Belgrade. Other cases involved military organizations of NATO-member states and individuals. Russia is an aggressive collector of information regarding NATO and NATO forces, including NATO PfP-member-states. It is a fact that since 1992/93 Open Source Intelligence could supply the majority of data without much HUMINT and TECHINT intelligence efforts. Realizing the easy access to such data, and the advantage of too much openness for antagonist governments and terrorist groups, the United States, NATO and many countries, have begun to limit the free flow of information.

[100] 5 U.S.C. 102, 5 U.S.C. 105, 42 U.S.C. 2011, 50 U.S.C. 1801, 18 U.S.C. App.1, EO 10450, EO 10865, EO 12333, EO 12356, EO 12958, EO 12968 (*Classified National Security Information*). Especially EO 12333 (*United States Intelligence Activities*, 1981), EO 12356 (*Uniform System for Classifying, Declassifying and Safeguarding National Security Information*, 1982), and EO 12968 (*Access to Classified National Security Information*, 1995) were important guidelines for NATO.

[101] Overall guidance by the *National Interest* and the interests of the United States, its institutions and citizens; access to classified information; security policy guidelines; *Need for Access*, *Need to Know*-policy; Security Policy Board, Nondisclosure Agreement; list of employees with access to classified information; reinvestigation, employee education and acceptance rules. For the mutual interests of U.S. and NATO to safeguard classified information see: Herbert Lewis: Safeguarding Classified Information, Defense Management Journal, Oct. 1973, pp. 29-31 and p. 62, and other recently updated literature.

[102] A number of states will only obtain papers classified as NATO *Confidential*, many PfP states are only eligible for NATO *Restricted* data. Material, which is *Confidential* or higher, is only released on a *Need to Know-Basis* to an individual with a specific c*learance*, whereas some non-classified material is distributed freely which includes a large number of STANAGs for information purposes.

[103] Rumsfeld Urges NATO Intelligence Coordination. 9 Feb. 2004, U.S. Department of Defense News Briefing, of Secretary of Defense Donald H. Rumsfeld, Feb. 7, 2004, 6 pages.

[104] According to the *Atomic Act* (1954, PL 585, Sect. 123 and 144) the classifications were: US Citizens Only, No Foreign Government (NOFORN), Specified Countries Only, Dissemination Only with Consent of Originating Agency (ORCON, EO 12958); the document classifications were: Official Use Only, Restricted, Confidential, Secret, Top Secret. According to DoD Directive 5100.55 the classifications were extended to Cosmic Top Secret (CTS). NATO identified its documents by adding "NATO": NATO Top Secret, NATO Secret, NATO Confidential, NATO Restricted. Nuclear documents received the term Atomic Material (ATOMAL). In the U.S. additional restrictions were eliminated in 2004 like: Warning Notice Intelligence Sources or Methods Involved; Warning Notice Sensitive Sources and Methods Involved, Controlled Dissemination Only, NSC Participating Agencies Only, Intelligence Components Only, No Dissemination Abroad, Background Use Only, USIB Only, NFIB Only, and the classification "Limited". The CIA had for a number of years its own classifications system with UMBRA. NOFORN, NOCONTACT, PROPIN and ORCON. See: International Security Handbook, Chapter 10: North Atlantic Treaty Organization (NATO) Security Procedures, Office of the Deputy to the Under Secretary of Defense for Policy Support, Washington, DC, 1993. See also: Walter Pincus: Keeping Secrets: In Presidential Memo, A New Designation for Classifying Information, Washington Post, May 19, p. A 15.

[105] NATO Facility Clearance Certificate.

[106] Andrew Scutro: Photo Sparks Imagery Debate, Defense News, Aug. 20, 2007, p. 8.

[107] Many cases: The last one involved the New York Times about a secret CIA directive to kill terrorists on foreign soil. See: Eli Lake, Sara A. Carter: CIA asks Justice to probe leaks of secrets, The Washington Times, Sept 4, 2009. See also: Barbara Starr, Peter Benson: Source: CIA hired Blackwater to hunt al Qaeda leaders, CNN.com/US, Aug. 20, 2009; Mark Mazzetti: C.I.A. Had Plan to Assassinate Qaeda Leaders, The New York Times, July 13, 2009. p. A1; Karl Rove: It's Dangerous to Give Congress Information, Fox News, with Bill O`Reilly, July 14, 2009. Seymour Hersh reported that the killing was done by Navy SEALs, CIA, Delta Force etc., a statement that was mostly fabricated. U.S. citizen turned terrorist were in 2009 on the "hit-list" of the CIA.

[108] This involved even Senator Patrick J. Leahy, a former Vice Chairman of the Senate Select Committee on Intelligence, and the Chief of Staff of Vice President Cheney, I. Lewis Libby. President Obama therefore decided (like President Bush before him) to maintain strict rules in regard to sensitive information, which even includes withholding such information from members of Congressional committees. See: Walter Pincus: House votes to revise intelligence disclosure rules for president. The Washington Post, March 2, 2010, page A1. Congress passed a law that requires the President to inform Congress, but with the exception of "special situations". But it is up to the President to decide what such a "special situation" would be, and he must not inform the whole committees.

[109] Rudolf Adam: Kenne dich – und kenne den Feind. Die Bedeutung nachrichtendienstlicher Aufklärung für Auslandseinsätze, Terrorabwehr und globaler Krisenbewältigung, IP, Mai 2007, pp. 43-51.

[110] Kevin O'Brien: Europe weights up intelligence options, Jane's Intelligence Review, March 2001, pp. 20-23, Ole R. Villadsen: Prospects for a European Common Intelligence Policy, Center for the Study of Intelligence, Studies in Intelligence Summer 2000, pp. 81-94

[111] See also: Svend Bergstein: Beitrag der Nachrichtendienste zur europäischen Verteidigung, pp. 319-335, in: Karl von Wogau: Auf dem Weg zur Europäischen Verteidigung. Verlag Herder, Freiburg im Breisgau, 2003.

[112] Alexander Siedschlag: Innenpolitische Entscheidungsprozesse bei Streitkräfteeinsätzen im Rahmen der Petersberg-Aufgaben der Europäischen Union – Deutschland, Frankreich, Großbritannien, Italien, Schweden. Studie im Auftrag der Stiftung Wissenschaft und Politik, Juli 2001.

[113] See the report about the EU Joint Situation Center by Jelle van Buuren: Secret Truth. The EU Joint Situation Centre, Amsterdam 2009. This report was considered as a severe breach of security. See also: Martin Walker: Bringing Intelligence To The Europlex Will Be A Real Coup, UPI, Aug. 18, 2008.

[114] Nicholas Fiorenza: NATO plans for more operations, JDW, 14 June 2006, p. 6; NATO plans summits to map out its future shape as deployed operations increase, Jane's International Defense Review, Jan. 2006, pp. 12-13; Jaap de Hoop Scheffer: Beyond the Borders. NATO Must Take Broader Global Perspectives Defense News, Nov. 15. 2004, p. 29.

[115] Pierre Claude Nolin, (as General Rapporteur (of the) NATO Parliamentarian Assembly, 2004 Annual Session): 177 STC 06E – Interoperability: The Need for Transatlantic Harmonization, discussing airlift, air defense, Network Centric systems, force protection, missile defense, precision munitions, tanks and fighting vehicles, intelligence, surveillance and reconnaissance, satellites, sensors, AWACS, UAVs, communications, C2, technology transfer from the US to European forces, GPS and Galileo, C4ISTAR and a New Strategic Concept for 2010.

[116] Donald C. Daniel: NATO Technology: from Gap to Divergence? Defense Horizons, No. 42, July 2004, Center for Technology and National Security Policy, National Defense University, Washington, DC, 2004.

[117] Nancy Bernkopf Tucker: The Cultural Revolution in Intelligence: Interim Report. The Washington Quarterly, Spring 2008, pp. 47-61.

[118] Richards J. Heuer: Limits of Intelligence Analysis, Orbis, Winter 2005, pp. 75-94.

[119] This underlines the importance of separate estimates. But politics can influence or pre-determine the analysis as well.

[120] Surprises are an ingredient part of politics, economies, sciences and therefore also of intelligence and warfighting. The best intelligence services will have their share of wrong predictions, like the often-quoted failure of Israel to detect the preparations of Egypt in the summer of 1973 to attack Israel in October. The Soviet Union had ion 1940/41 a large network of spies in Germany (including the Außenamt), but they did not assess properly the huge and well visible build-up for *Barbarossa*, because the mindset of the Communists, the NKVD and Stavka was fully engulfed by the German-Soviet treaties signed in 1939.

[121] Sandra I. Erwin: War Lessons Should Not Be Politicizied, Says CENTCOM Chief, National Defense, March 2004. See also the comments when the U.S. intelligence community presented their conclusive *Iran: Nuclear Intentions and Capabilities*, National Intelligence Estimate, November 2007, on Dec.3 (without the confidential parts).

[122] This led in 2001 to wrong conclusions by the White House, based on information and assumptions provided by an Iraqi low-key engineer about an ongoing nuclear weapons program, which did not exist.

[123] Over 300 articles were written on this subject in the late 1980s. See: Rose: Why Artificial Intelligence won't work, Military Technology/MILTECH 7/87, pp. 86-87.

[124] Rod Nordland: 25 Afghan Police May Have Joined Taliban, The New York Times, Feb. 19, 2010.

[125] Fixing Intelligence: A Blueprint for Making Intelligence More Relevant for Afghanistan. Voices from the Field. January 2010.

[126] Lawrence Sellin, UPI, Jan. 12, 2010

[127] Reuters, Washington, DC, Jan 5, 2010

[128] Quoted in: Fixing Intelligence: A Blueprint for Making Intelligence More Relevant for Afghanistan. Voices from the Field. January 2010. p. 4, 9.

[129] See: Edward Waltz: Information Warfare. Principles and Operations, Artech House, Boston, Mass., 1998.

[130] Sherman Kent: Strategic Intelligence for American World Policy. Princeton Univ. Press, Princeton, NJ, 1966.

[131] NATO Allied Command Operations, SHAPE, Joint Staff Branches; NATO Allied Land Component Command. See: http://www.nato.int/shape/about/structure.

[132] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[133] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[134] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[135] AJP-3.6 Allied Joint Electronic Warfare Doctrine; MC 64/9 NATO Electronic Warfare (EW) Policy.

[136] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006). HUMINT activities include espionage, military attaches, inerrogation and questioning of refugees, prisoners of war, diplomats,

[137] MC 402/1 NATO Policy of Psychological Operations.

[138] MC 422/1, NATO Information Operations Policy.

[139] Hanno Rank, Burkard Schmitt: The Challenge of Information Security, Military Technology/MILTECH 11/2005, pp. 50-57.

[140] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[141] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[142] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.

[143] Even the demand of Congressional oversight is often subject of criticism. Congress had in the past often leaked sensitive information because of lax security and there are no established standards in handling classified information. The demand of Congress to be informed on a prior-notification basis was later on declined and did not come up after the attacks on the U.S. Sept. 11, 2001. However, more devastating effects had books and articles written by former employees of the intelligence agencies and of journalists writing about internal procedures and foreign intelligence and counterintelligence operations. One of the largest breaks of "strategic intelligence" did occur when Daniel Ellsberg sent his collection of papers regarding the U.S. policy in Southeast Asia (and Vietnam) to the New York Times and Washington Post, later on published under the title *The Pentagon Papers*. The Ellsberg Case of 1969 had an impact on internal security, the EO 11652 (Classification of Documents, 1972) and the Civil Service Reform Act of 1978.

[144] Fixing Intelligence: A Blueprint for Making Intelligence More Relevant for Afghanistan. Voices from the Field. January 2010. p. 7.

[145] See: FM 2-22.3 Human Intelligence Collection Operations (2006), 5-12.

[146] See: FM 2-22.3 *Human Intelligence Collection Operations* (2006), 5-12.