Aleš Čretnik

Strokovni članek

ZDRUŽEVALNI CENTRI V PROCESU IZMENJAVE PODATKOV – PROBLEM ALI REŠITEV?

FUSION CENTRES IN INFORMATION SHARING PROCESS – A PROBLEM OR A SOLUTION?

Professional article

Povzetek Teroristični napadi 11. septembra v Združenih državah so postali katalizator sprememb v mnogih nacionalnih in celo mednarodnih obveščevalnih sredinah. Glavni cilji teh obveščevalnih reform so bili optimizirati sistem in ponovno osredotočiti obveščevalne aktivnosti na asimetrične grožnje, še posebej na terorizem. Sestavna in zelo pomembna sestavina boja proti mednarodnemu terorizmu je bila potreba po izmenjavi podatkov in sodelovanju, tako da je bilo oblikovanje nacionalnih in večnacionalnih združevalnih centrov logična posledica. Koncept združevanja podatkov ni nov pojav in bi moral biti sestavni del procesa zbiranja in izdelovanja v vseh obveščevalnih in varnostnih organizacijah. Vseeno pa so, na splošno, področja zanimanja v nacionalnih in večnacionalnih združevalnih centrih različna, saj se prvi običajno osredotočajo na notranjo, nacionalno varnost, drugi pa na trenutna in mogoča krizna področja, na države, ki so še posebej zanimive za večnacionalne združevalne centre, ter transnacionalne zadeve, kot so mednarodni terorizem, organiziran kriminal ter širjenje orožij za množično uničevanje. Iz nacionalnega vidika je najbrž spojitev obeh odgovornosti v okviru enega samega nacionalnega združevalnega centra idealna rešitev za pokrivanje širšega spektra potreb uporabnikov, posebno za manjše države z omejenimi človeškimi in finančnimi viri.

Ključne besede ***Obveščevalni združevalni center (IFC), asimetrična grožnja, obveščevalni podatki, izmenjava podatkov, združevanje, večnacionalni.***

Abstract The 9/11 terrorist attacks in the United States became the catalyst for changes in many national and even international intelligence communities. The main aims of these intelligence reforms were to optimize the system and re-focus intelligence activities towards asymmetric threats, especially terrorism. An integral and crucial component of the fight against international terrorism was the need for information sharing and cooperation, and the establishment of national and multinational fusion centres was a logical outcome. The concept of data fusion is not a new phenomenon

and should already be an integral part of the collection and production process of any intelligence or security organization. However, in general, areas of interest are different between national and multi-national fusion centres, as the former are usually focused on internal national security and the latter on current and potential crisis areas; countries of special interest in a multi-national fusion centre and trans-national issues such as international terrorism, organized crime and proliferation of weapons of mass destruction. From a national perspective, the merging of both responsibilities under a single 'national fusion centre' would probably be an ideal solution to cover a wider spectrum of the customers' needs, especially for smaller countries with limited human and financial resources.

Key words ***Intelligence Fusion Centre (IFC), asymmetric threat, intelligence, information sharing, fusion.***

Introduction

Since the disintegration of the Soviet Union and the end of Cold War in 1991, NATO has not been confronted with a direct conventional threat. The 9/11 events became the catalyst for changes, not only within the US intelligence community, but also in other national and international intelligence organizations. In many countries, the re-focus of intelligence activities has been towards asymmetric threats, international terrorism being the primary one. The main aim of these intelligence reforms was to optimize the system and minimize the possibility of future intelligence failures through changes in all phases of the intelligence cycle. Moreover, some responsibilities which had previously been exclusively within the competence of the police or special operations forces (SOF) have come under the jurisdiction of national intelligence organizations. An integral and crucial component of the combat against international terrorism was the need for information sharing and cooperation; it was also confirmed by the 9/11 Commission Report issued in 2004 (Anon., 2004). Before the 9/11 attacks, the report discovered that different intelligence agencies had dispersed relevant information, but due to the lack of inter-agency cooperation, had not properly shared, fused and analysed them. Therefore, an establishment of fusion centres, known also as intelligence fusion or information fusion centres, has become a logical consequence of the report. Furthermore, other nations and international organizations, such as NATO, have also positively received the idea.

The purpose of this article is to present the fusion concept and the importance of information sharing. It is divided into three parts. The first part examines the development of different types of fusion centres and their role in information sharing in national and multi-national intelligence and security environment. In the second part, the fusion centres' main characteristics are analyzed and in the third part, lessons learned are presented. In conclusion, the article exposes characteristics of a fusion centre that would probably be a suitable model at national level.

1 FUSION CONCEPT AND TYPES OF FUSION CENTRES

As asymmetric threats, such as terrorism, extremism and organized crime constantly endanger modern society, and the ability of the respective national and international agencies to share information and intelligence has become critical. Timely and accurate intelligence plays a key role in prevention and response to asymmetric threats. Due to obtaining information from various sources, fusion becomes an essential process in transforming the data into actionable intelligence that facilitates the decision-making process.

The concept of data fusion is not a new phenomenon and should already be an integral part of the collection and production process of any intelligence or security organization. In addition, fusion centres had existed in the US and elsewhere before 2004, yet they did not have the word 'fusion' in the title. For instance, as the product of counter-drug initiatives in the 1980s, early intelligence fusion centres, referred to as Regional Intelligence Centres (RIC), had the same role as the 'new' fusion centres – to analyze all available information (Carter, 2007).[1] The most important part of 'new' fusion centres which is constantly stressed is the need to share information with elements inside and also outside a single intelligence organization or community, for instance with other countries, organizations, private security companies, etc., and to process it into all-source intelligence products (Anon., 2006). Due to the fact fusion centres do not have indigenous collection capabilities, but are analysis-driven support centres, they fully depend on information provided. As information sharing has actually become the main part of fusion centres, they encourage cooperation at national and even international level. Therefore, there is an interesting question of why nations and international organizations have established fusion centres, when the concept had already been known before the 9/11 attacks. Is a fusion centre just a new 'shiny intelligence structure' with the already known concept? It can be argued that the period after the 9/11 events has probably presented the right momentum for nations and international organizations to modernize intelligence structures and emphasize and prepare legal frameworks for proper information sharing; this has actually changed the 'need-to-hide' or 'need-to-know' principle to a 'need-to-share' principle. The change has been especially important at national level. For example, within the US intelligence community, the protection of sources, methods, stove piping of raw intelligence, and also their strict application of the 'need-to-know' rule in order to avoid sharing information with other national agencies, has been a hindrance to information sharing especially between the CIA and FBI (Goodman, 2003:64). This became officially acknowledged after the National Commission inquiry reported on the 9/11 events. Because of poor collaboration, there was no link between domestic and foreign intelligence; in other words, the 9/11 planning fell into this void between the CIA and FBI. While the FBI looked for sleepers' cells, the CIA focused on possible overseas threats to the US interests. Consequently, nobody

[1] *There are many other examples of 'fusion' centres that were established in the past, but it is not necessary to focus on all of them for the purposes of this article.*

focused on the foreign threat to domestic targets and therefore ignored foreigners who had infiltrated and then attacked the US (Gill & Phythian, 2008:119-120).

Fusion centres are divided based on their area of interest (foreign and domestic intelligence), and on the number of nations that contribute personnel to a centre (national and multi-national) (Carter, 2007). National fusion centres focus mainly on internal security issues and have a capability of blending law enforcement information and intelligence. Their main purpose is to bring all relevant partners together to maximize the capability to identify, thwart and respond to terrorism and criminal acts (Anon., 2006). They should fuse foreign and domestic intelligence across all levels and sectors of government and private sector in order to support policymakers (Willis & Lester & Treverton, 2009:353).[2] Multi-national fusion centres are actually intelligence fusion centres that can have a broader spectrum of responsibilities and are mainly focused on collation, processing and analysis of foreign intelligence concerning current and potential crisis areas, as well as countries of special interest to a multi-national organization. For the latter, terrorism is not necessary their main focus, yet it is part of a full intelligence support to their customers.

From 2004, many fusion centres were formed in the US, Canada, United Kingdom, some other countries, and at ISAF in Afghanistan; within ISAF, several intelligence fusion centres were formed at a tactical level, for example Kandahar Intelligence Fusion Centre (KIFC). In addition, the US have had a primary role as a framework nation in establishing two multi-national intelligence fusion centres, the main tasks of which are collation, processing and analysis of intelligence, and production of final intelligence products in support of military operations. The first one of them, established in Bahrain, January 2005, was the Combined Naval Forces Central Command Coalition Intelligence Fusion Centre (CENTCOM CIFC). The second one is the Intelligence Fusion Centre (IFC) in support of NATO, established at RAF Molesworth, United Kingdom, in October 2006.

Intelligence reforms after the 9/11 terrorist attacks, such as restructuring of existing national and international intelligence systems, greater competence and authority of intelligence and security organizations in terms of collection of domestic and foreign intelligence, have influenced the forming of fusion centres. They do not replace existing national and international intelligence structures, but should complement them. Centres present a hub where ideally all relevant information and intelligence received is analyzed and provided in a timely manner to their customers. For example, US fusion centres, established at state and local level, use capabilities and resources of US intelligence and law-enforcement agencies, but their area of interest is local. Most information and intelligence is provided to fusion centres by local and/or state security and law-enforcement organizations, and the private sector. However, an additional intelligence source is security and intelligence organizations

[2] *The private sector can be a good source of information and at the same time is often a legitimate consumer of law enforcement information, as it is a large percentage of the critical infrastructure owned by the private sector (Carter, 2007).*

at the federal level. Another example is the IFC which fuses relevant information and intelligence that exists inside NATO and provides intelligence products mainly at the strategic and operational level but also, to a lesser extent, at the tactical level. The IFC is a Memorandum of Understanding (MoU) organization and it is not part of the NATO formal peace establishment structure (PE structure). That means that when it was established it did not replace the existing NATO intelligence structure or any element in it. More discussions of the differences in the fusion centres' role and authority, especially between national and multi-national ones, follow.

1.1 National fusion centres

1.1.1 Fusion centres in the US

In 2004, many US states and large cities established state-level and local fusion centres for sharing information and intelligence within their jurisdictions as well as with the federal government. They have received funds from federal, state and local levels, as well as from the Department of Homeland Security (DHS), which paid more than $254 million between 2004 and 2007 in support of these centres. As of July 2009, there were 72 designated fusion centres around the country, with 36 DHS field representatives deployed (Anon., 2009c). Employed in the fusion centres are personnel from federal, state and local intelligence and security agencies; police; public safety agencies, such as fire, health and transportation; and the private sector (Anon., 2006).

1.1.2 US National Counterterrorism Center (NCTC)

Established in August 2004, the National Counterterrorism Center (NCTC) currently has around 500 personnel from more than 16 federal departments and agencies. Organizationally, it is part of the Office of the Director of National Intelligence (ODNI). NCTC is the primary organization in the US for analyzing all intelligence pertaining to counter-terrorism (CT). It incorporates all analysis from across the Intelligence Community and produces intelligence assessments to support policymakers and other customers from the political, intelligence, law enforcement, defence, homeland security, and foreign affairs communities. It is also responsible for an evaluation of CT analytical production and training of personnel. Moreover, it presents a knowledge bank on known and suspected terrorist groups and their associated individuals. In the NCTC, around 30 classified information-communications systems are co-located, owned by intelligence, military, law enforcement and homeland security to facilitate information sharing (Anon., 2009a).

1.1.3 British Intelligence Centre[3]

In April 2009, the British Ministry of Defence announced that it would spend £150m on merging some military intelligence units at RAF Wyton, Cambridgeshire. The project, which should be finished by 2012, will provide modern and flexible accommodation for approximately 1,100 military intelligence employees. Headquarters

[3] *'British Intelligence Centre' is not the official name of this future organization.*

Intelligence Collection Group, currently based in Feltham, Middlesex, and sub units – the National Imagery Exploitation Centre (also known as JARIC), currently at RAF Brampton; the 42 Engineer Regiment (Geographic), currently based at Hermitage near Newbury and Germany, will be moved into the new intelligence centre (Anon., 2009b). This project will form a hub for GEOINT collection and analysis and will enable the organization to deliver a more effective GEOINT support to military and, to some extent, to CT operations. The centre does not present a standard all-source intelligence fusion centre, as it will only merge GEOINT elements. Therefore, there is an assumption that all-source intelligence analysis is highly likely to remain in the domain of Defence Intelligence Staff (DIS) in London, while the Government Communications Headquarters (GCHQ) in Cheltenham, Gloucestershire, will provide SIGINT.[4]

1.2 Multinational fusion centres

1.2.1 Combined Naval Forces Central Command Intelligence Fusion Cell (CNFC/CIFC)

In January 2005, CENTCOM's Maritime Component Commander established a multinational intelligence organization – the Coalition Intelligence Fusion Center (CIFC), located in Bahrain. At the beginning, the centre had a staff of about 15 naval personnel from about 12 countries. In combating terrorism, the nation's support of the maritime aspect was to provide ships and supplies, and analysts working in the CIFC, which provides vessels of combined task forces the actionable intelligence on terrorists or other illegal network activities (Raman, 2005; Garamone, 2006).

1.2.2 Intelligence Fusion Centre (IFC) in Support of NATO

The IFC, a multi-national intelligence organization, was officially established in October 2006. A year later, it was declared to have full operational capability. Initially, IFC's workforce was going to be approximately 162 personnel, but the centre is still developing and it will likely number more than 200 personnel in the near future. As of December 2009, 24 NATO member nations pledged to fill available positions in the IFC (Anon., 2008).

The IFC does not have its own collection capabilities and therefore relies fully on national and partners' intelligence, and intelligence from areas of NATO operations. Moreover, because it shares its location with the US European Command Joint Analysis Center (USEUCOM JAC) and the US Africa Command Joint Intelligence Operations Center (USAFRICOM JIOC), it also has a great opportunity to collaborate with both US centres. Intelligence analysts working in the Operational Intelligence Centre, Analysis Division, and Operational Support Division fuse information and intelligence provided by open source intelligence (OSINT), signals intelligence (SIGINT), human intelligence (HUMINT), geospatial intelligence (GEOINT), and Measurement and Signatures Intelligence (MASINT) (Anon., 2007;

[4] *For more information on the GCHQ see http://fas.org/irp/world/uk/gchq/index.html, 8 Dec 2009.*

Mixon, 2007).[5] SIGINT, GEOINT and MASINT are provided by NATO member nations, as NATO does not have these indigenous intelligence collection means. NATO has its own HUMINT capabilities only in its areas of operations, such as Bosnia, Kosovo and Afghanistan. Sharing final intelligence products via classified information-communications systems – e.g. BICES – with NATO Allies and partner nations and organizations, thereby improves intelligence support to the SACEUR, NATO and NRF operations.[6] The IFC responds to Requests for Information (RFIs) sent by the SHAPE J2, ISAF and KFOR commanders. The IFC is transforming the way NATO intelligence structures support operational forces and is proving to be the recognized model for international support and cooperation. Most importantly, the IFC is a significant contributor to combating terrorism. Intelligence analysts produce strategic and operational terrorist threat assessments, high value individual psychological profiles and target's packages, GEOINT products for planning and execution of SOF operations in crisis areas, etc. (Anon., 2008). The US National Geospatial Intelligence Agency (NGA) is a great supporter of the IFC as it provides its own analysts and geospatial data to the centre (Eilenberger, 2009). In addition to SOF, ISAF and KFOR Headquarters, Allied Command Counter Intelligence (ACCI) and the NATO Office of Security (NOS) are among main customers of CT-related intelligence products.[7]

2 COMPARISON OF NATIONAL AND MULTINATIONAL FUSION CENTRE

The following text compares a generic US National Fusion Centre and the IFC in support of NATO. The purpose of the comparison is to discover what type of fusion centre is more appropriate and efficient in providing intelligence support to decision makers. Thereby, it is important to understand the role and characteristics of national and multinational fusion centre.

Characteristics of the US National Fusion Centre:

- It is an analytical body and usually does not have its own intelligence collection sources;
- Personnel are from different US national intelligence, security, law enforcement organizations, the police and even the private sector;
- Ideally, the organization should operate on one national classified information-communications system, but in practice, many organizations involved have their own networks, and personnel from a certain organization that work in a fusion centre and check their organization's network for specific information. This is necessary due to privacy, human rights and civil liberties of US citizens. In

[5] *For more information about intelligence collection sources see Schulsky, 2002:11-40.*

[6] *BICES - Battlefield Information Collection and Exploitation Systems.*

[7] *ACCI is the only organic Counterintelligence (CI) unit assigned to NATO. In 2008, it consisted of representatives from 17 Allied nations. ACCI is responsible for protection of Allied Command Operations (ACO) and Allied Command Transformation (ACT) formations from Terrorism, Espionage, Sabotage, and Subversion (TESS). ACCI executes its mission anywhere NATO troops are assigned or deployed. For more information, see http://www.shapeonline.net/articles080610/Allied-Command-Count.html, accessed on 8 Dec 2009.*

general, the organization should have access to all available information provided by national intelligence, security, and law enforcement organizations; foreign partners' intelligence can be provided on request or through bilateral cooperation;
– As it is focused on internal security, it fuses law enforcement information and national intelligence, and provides mostly actionable intelligence to its consumers at local, state or even federal level;
– It can ask US national intelligence, security and law enforcement organization for additional information;
– It responds to customers' requests for information.

Characteristics of the Intelligence Fusion Centre (IFC):
– It is an analytical body and does not have its own intelligence collection sources.
– NATO member nations that signed the MoU provide personnel for limited periods, usually for three years.
– National and multi-national intelligence is uploaded on a single NATO classified information-communications system (BICES). It presents the main network for the IFC.
– It fuses only intelligence and not law enforcement information. Intelligence provided by nations, partners, operations' and other NATO headquarters. As the IFC is an intelligence organization and not law enforcement or police organization, its products regarding CT can be used only for identifying terrorist groups, networks and associated individuals, and assessing their intentions and capabilities. They are not admissible in court.
– It has the authority to ask NATO nations for additional information and responds to customers' RFIs.
– It collates, processes, analyses and assesses provided intelligence and information. IFC provides timely, accurate, and sometimes actionable strategic, operational and even tactical written and graphic intelligence products to SACEUR, NATO operations and other customers in NATO. Occasionally, it releases its intelligence products to other international operations or organizations, like the EU.
– Planning of collection and production is based on strategic guidelines and intelligence requirements provided by main customers.
– There are no constraints on establishing and maintaining cooperation and sharing of information with external partners, such as non-member countries, international organizations, etc.

3 FUSION CENTRES AND LESSONS LEARNED

Lessons learned have exposed some positive aspects of establishment of fusion centres; however, some issues still remain unsolved, such as information sharing, lack of relevant intelligence and dissemination of final intelligence products. Fusion centres have proved to be an important part of intelligence but they cannot eliminate all anomalies that exist in intelligence communities. In the case of IFC, NATO finally has an intelligence element that can directly support NATO operations, SACEUR and other customers. Despite the fact that IFC is not a part of the PE structure,

ISAF and KFOR rely on it, because in the last three years IFC has proved to be a credible partner. IFC has acknowledged that liaison with main customers is crucial in intelligence, therefore, it sends liaison officers to KFOR on regular basis and it has a permanent liaison officer to ISAF. These officers coordinate requests for information and IFC responses, and at the same time they identify issues that hamper an effective intelligence support to operations. For example in ISAF, several deficiencies have been identified not only by IFC but also by current ISAF CJ2 Chief Major General Michael T. Flynn. Fusion centres can fuse and analyze only information and intelligence that is provided to them, and when they are given poor information at the beginning, the analysis will likely be poor as well – the 'garbage in, garbage out' phenomenon. In case of ISAF, General Flynn has exposed that a lot of unclassified and classified information that is at grassroots level never reaches intelligence analysts due to severe technological hindrances, like multiple secret networks and lack of databases (Flynn, Pottinger, Batchelor, 2010:14). In addition, there is also lack of diplomatic reports from NATO civilian representatives and specific national intelligence, which can significantly increase the quality of IFC intelligence products. Another still existing problem, probably not encountered only by the IFC, is dissemination of final products to customers, which despite the 'need-to-share' principle do not always reach all relevant customers. Reasons for that are already mentioned multiple secret networks, low bandwidth, incomplete e-mail distribution lists, limited access to NATO dissemination tool, etc. Protection of classified data does not hamper dissemination of intelligence products, and it can be said that it does not present any challenge for the IFC, as the organization can obtain and provide all classified information via BICES. The same can be stated for classified information that is obtained through national classified systems in 'country rooms' and uploaded on BICES.

However, fusion centres can actually become a problem when there are too many of them inside one intelligence community in addition to already existing intelligence and security organizations. For instance, in the US, in addition to 16 national intelligence agencies, there are 72 fusion centres and some states have even up to eight of them (Rollins, 2008:20). Intelligence community becomes too complex and the collection, cooperation and analysis are less transparent. Despite the fact, these fusion centres are focused on local security issues, and their areas of responsibility are often overlapping. A similar situation can be seen in Afghanistan, where there exist ISAF HQ J2/G2/S2 intelligence structure, national intelligence cells and units, regional intelligence fusion centres, and other elements that collect and analyze collected information. In these cases, it is not transparent who does what, and instead of fusion there is confusion in the intelligence system.

Conclusion

This article has examined the different types of fusion centres. In terms of countering asymmetric threats the comparison speaks in favor of national fusion centres, which provide actionable intelligence and can prevent, in cooperation with law-enforcement and police, illegal acts in time and the perpetrators/suspects prosecuted.

However, the national fusion centre as described above does not necessary represent an ideal solution as it usually only covers threats within a country.

In the last decade, asymmetric threats have posed a growing problem for the troops deployed within the framework of a military operation. More importantly, criminals, extremists or terrorists from such areas of operations as Afghanistan, Bosnia or Kosovo have often kept contacts or even travelled to the states that have troops deployed in their countries of origin and want to execute illegal activities there. To prevent an information flow gap between national intelligence elements involved in a military operation abroad and national security organizations at home, a single 'hybrid' national fusion centre would probably be an ideal solution to cover a wider spectrum of customer's needs, especially for smaller countries with limited human and financial resources. Such fusion centres would have sources, capabilities and responsibilities of both of the compared centres. The advantage of having a single fusion centre is that it might be easier to ensure transparency of coordination and sharing of information among organizations that are part of a national intelligence and security system. The centre's subordination would depend on the respective state's constitutional model, but in most cases would be subordinate to the Prime Minister. The centre would consolidate efforts of national security, intelligence, law enforcement, the police, private sector and other organizations which could contribute to national security, prevention of foreign intelligence activities and force protection of deployed military and police troops to multi-national operations. In other words, the fusion centre would merge domestic and foreign intelligence. The organizations whose representatives would work in the centre would continue with their regular activities and the centre would work on interdepartmental tasks, where more organizations could provide information to solve a certain problem. In this case, organizations' representatives present a liaison between the centre and indigenous organizations, their partner countries and multi-national organizations. Ideally, all of the involved national elements, including the centre, would have access to a single classified information-communications system, where all information based on the principles of 'need-to-know' (access to databases with personal data) and 'need-to-share' are available.

However, the centre would need effective oversight in order to prevent the legalization of potential centre's illegal activities and politicization of intelligence, and also to control and oversight of handling data, budget, quality of analysis, legality, propriety and efficacy of centre's activities, its responsiveness, destruction of archives, human rights and civil liberties, and ethics (Lowenthal, 2009; Gill & Phythian, 2008). As the centre presents an analytical, and not intelligence collection asset, oversight has to focus mainly on accessing, processing and archiving of personal data, and to determine the centre's accountability with regard to human rights and civil liberties. Human rights and civil liberties present a very delicate issue, especially in those countries that used to have a secret police or service collecting information on citizens and 'an internal enemy' with the purpose of protecting a regime. Therefore, strict legislation and efficient control and oversight of the fusion centre and its

accountability, are mandatory to protect rights and civil liberties of citizens, but at the same time to counter threats to national and international security in an appropriate legal way.

To conclude, intelligence fusion centres present a relatively new trend initiated by the events of 9/11. Sharing of intelligence still presents an issue in many countries; fusion centres can eliminate some of the obstacles but cannot eliminate them all. The 'need-to-share' principle is especially important in countering asymmetric threats, where timely intelligence, which is possible to act upon, can save many lives. Finally, intelligence can be actionable only if an action is taken, and for that it is very important to have national legislation that is able to deal with national security effectively and, at the same time, protect the rights and civil liberties of individuals.

Bibliography

1. *Anon., 2004. The 9/11 Commission Report. The 9/11 Commission Website. www.9-11commission.gov/report/911Report.pdf , 11 April 2009.*
2. *Anon., 2006. Fusion Center Guidelines – Developing and Sharing Information and Intelligence in a New Era. Washington DC: The U.S. Department of Justice's (DOJ) Website. http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf, 11 December 2009.*
3. *Anon., 2007. Statement of Work for NATO Intelligence Fusion Cell Intelligence Analytical Support. Ramstein: The Ramstein Air Base Website. http://www.ramstein.af.mil/shared/media/document/AFD-071213-025.pdf, 6 December 2009.*
4. *Anon., 2008. IFC General Information Template (unpublished). Molesworth: Intelligence Fusion Centre (IFC) in support of NATO.*
5. *Anon., 2009a. About the National Counterterrorism Center. National Counterterrorism Center. http://www.nctc.gov/about_us/about_nctc.html, 6 December 2009.*
6. *Anon., 2009b. £150m to merge intelligence centres. www.defencemanagement.com in association with Defence Management Journal. http://www.defencemanagement.com/print_news.asp?type=news&id=9381, 6 December 2009.*
7. *Anon., 2009c. State and Local Fusion Centers. Department of Homeland Security. http://www.dhs.gov/files/programs/gc_1156877184684.shtm, 1 December 2009.*
8. *Carter, David l., 2007. The Intelligence Fusion process for State, Local and Tribal Law Enforcement. Michigan: Michigan State University. http://www.cops.usdoj.gov/files/ric/CDROMs/LEIntelGuide/pubs/IntelligenceFusionProcessWhitePaperv3.5.pdf , 13 December 2009.*
9. *Eilenberger, Dawn, 2009. GEOINT Serves NATO. Washington DC: National Geospatial Intelligence Agency, https://www1.nga.mil/Newsroom/Pathfinder/0702/Pages/GEOINTServesNATO.aspx, 8 December 2009.*
10. *Flynn, Michael T., Pottinger, Matt, Batchelor, Paul D., 2010. Fixing Intel: A Blueprint for Making Intelligence Relevaent in Afghanistan. Washington, D.C.: Center for a New American Security. http://www.cnas.org/files/documents/press/AfghanIntel_Flynn_Jan2010_code507_voices.pdf , 7 January 2010.*
11. *Gill, P., Phythian, M., 2008. Intelligence in an Insecure World. Cambridge: Polity Press.*
12. *Goodman, M. A., 2003. 9/11: The Failure of Strategic Intelligence. Intelligence and National Security, 18 (4. Str., 59-71.*
13. *Lowenthal, M. M., 2009. Intelligence from Secret to Policy (Fourth ed.). Washington DC: CQ Press.*
14. *Mixon, Laurence M., 2007. Requirements and Challenges Facing the NATO Intelligence Fusion Center. Montgomery: Air University Research Information Management System.*

https://www.afresearch.org/skins/rims/q_mod_be0e99f3-fc56-4ccb-8dfe-670c0822a153/q_act_downloadpaper/q_obj_9a47b0f3-9dcb-41d3-b677-79544cdd6921/display.aspx?rs=enginespage , 4 September 2009.

15. *Rollins, John, 2008. Fusion Centers: Issues and Options for Congress. Federation of American Scientists. http://www.fas.org/sgp/crs/intel/RL34070.pdf, 11 January 2010.*
16. *Willis, Henry H., Lester, G., Treverton, G. G., 2009. Information Sharing for Infrastructure Risk management: Barriers and Solutions. Intelligence and National Security , 2 (3). ,Str. 339-365.*