RESEARCH PAPER
No. 100

June 2006

A (R)EVOLUTION IN INTELLIGENCE AFFAIRS? IN SEARCH OF A NEW PARADIGM

Dr. Andrew N. Liaropoulos

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

 # 1, Kalavryton Street, Ano-Kalamaki, Athens, 17456, Greece
RIEAS URL:http://www.rieas.gr

RIEAS MISSION STATEMENT

Objective

The objective of the Research Institute for European and American Studies (RIEAS) is to promote the understanding of international affairs. Special attention is devoted to transatlantic relations, intelligence studies and terrorism, European integration, international security, Balkan and Mediterranean studies, Russian foreign policy as well as policy making on national and international markets.

Activities

The Research Institute for European and American Studies seeks to achieve this objective through research, by publishing its research papers on international politics and intelligence studies, organizing seminars, as well as providing analyses via its web site. The Institute maintains a library and documentation center. RIEAS is an institute with an international focus. Young analysts, journalists, military personnel as well as academicians are frequently invited to give lectures and to take part in seminars. RIEAS maintains regular contact with other major research institutes throughout Europe and the United States and, together with similar institutes in Western Europe, Middle East, Russia and Southeast Asia.

Status

The Research Institute for European and American Studies is a non-profit research institute established under Greek law. RIEAS's budget is generated by membership subscriptions, donations from individuals and foundations, as well as from various research projects. The Institute is autonomous organization. Its activities and views are independent of any public or private bodies, and the Institute is not allied to any political party, denominational group or ideological movement.

John M. Nomikos
Director

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES (RIEAS)

Postal Address:

1, Kalavryton Street
Ano-Kalamaki
Athens, 17456
Greece

Tel/Fax: + 30 210 9911214

E-mail: rieas@otenet.gr

RESEARCH INSTITUTE FOR EUROPEAN AND AMERICAN STUDIES

(RIEAS)

RESEARCH PAPER
No. 100

June 2006

A (R)EVOLUTION IN INTELLIGENCE AFFAIRS? IN SEARCH OF A NEW PARADIGM

Dr. Andrew N. Liaropoulos

Abstract

This paper examines the challenges that the Intelligence Community is facing in the post Cold War era. The argument for an intelligence reform has always been popular, but gained greater momentum after 9/11. In order to define the argument for a Revolution in Intelligence Affairs, the paper examines several aspects that relate to intelligence reform, like the impact of information technology on the culture of intelligence, the open source solution, the problems regarding information overload and the politicization of the intelligence product. The purpose is to identify the dilemmas that reformers face and conclude on whether a new paradigm in intelligence affairs is about to emerge.

Table of Contents

A (R)EVOLUTION IN INTELLIGENCE AFFAIRS? IN SEARCH OF A NEW PARADIGM

1. Introduction

Recent developments like the 9/11 terrorist attacks and the politicization of intelligence in the case of the war in Iraq, have placed intelligence and its (mis)use by politicians, at the heart of the political debate. In the dawn of the twenty-first century, the international environment has been transformed and is more complex compared to the one that shaped the intelligence services during the second half of the twentieth century. In particular, whereas the Cold War provided a reasonably predictable and linear framework for the intelligence community, that can not be argued for the security environment at the beginning of the twenty-first century. Requirements for providing intelligence support have changed greatly. There is greater complexity and variety of enemies and threats. The linear understanding that characterized most of the intelligence issues during the Cold War is long gone. In the post 9/11 security environment there is a great need to re-examine the way intelligence is collected and translated into policy.

A number of intelligence scholars refer to the emergence of a new paradigm in intelligence affairs. The claims for openness and transparency of the intelligence process have been increased in the post 9/11 period and some scholars question whether intelligence reflects the needs and norms of the current open and post-modern western societies. [1] Others stress the importance of Open Source Information and examine the application of a new organisational paradigm that drives its inspiration from the business sector. [2] Piled together, they question the traditional way in which intelligence used to perform until the end of the Cold War and highlight certain aspects of a new and revolutionary intelligence model that is about to emerge. [3]

As a result, a provocative set of questions has been raised from the relevant literature. Is there a Revolution in Intelligence Affairs (RIA) already under way or is it just the latest catchphrase? How will the Intelligence Community adapt to the changes that globalisation, postmodernism and risk society brought about? Have certain aspects, like Open Source Intelligence (OSINT) or Human Intelligence (HUMINT), been overlooked by reformers? What are the advantages and disadvantages of outsourcing intelligence to the private sector?

2. The Argument for a Paradigm Shift in Intelligence Affairs

2. 1 Information Revolution and Intelligence

The Information Revolution challenges every bureaucratic institution and the intelligence services can not escape from this reality. The Information Revolution affects every step of the intelligence cycle; it adds new issues in the intelligence agenda, alters old ones and brings profound organisational and cultural changes in the art of intelligence. [4] The numerous proposals to reform and reorganise the intelligence community reflect the need to move from a hierarchical, stove-piped and inflexible system towards a new system. This new intelligence model will have to make the best of the available information means (information technology, open source intelligence), adopt new analytical tools and manage information overload in order to gain flexibility and provide sound analysis and timely 'early warning' indicators. A clear sign of the problems that the traditional, Cold War intelligence model had in adjusting to its new mission, is the tendency since the late 1990's to establish ad hoc task forces and intelligence centres. For example the U.S Intelligence Community has created new intelligence centres and organisations like the National Counterterrorism Center (NCTC), the National Counterproliferation Center (NCPC), the Terrorist Threat Integration Center (TTIC) and the Open Source Center (OSC), not to mention the establishment of the Department of Homeland Security (DHS), or created new posts for better coordination like the National Intelligence Director (NID) and the Undersecretary of Defense for Intelligence (USDI).

Information Technology has brought about new capabilities in the field of decentralization, tailored systems and networking. Instead of having a large number of users depend on a small number of centralized sensors or data processing systems, low cost, high capability sensors and microcomputers make it possible for many users to have access to their own data systems and tailor the equipment to the specific need of each user. In addition, communication links and software provide through Internet the necessary interconnectivity, so that individual users can share and exchange data. [5] Electronic dissemination has replaced the 'push' architecture, where the analysts select from a vast quantity of data, the information they believe the users need to know and then send this information to the users they believe need to have it, with the 'pull' architecture, where the users will draw the information they believe they need from the vast amount of data. [6]

Nevertheless, Information Revolution has also brought new vulnerabilities in the practice of intelligence. The growing dependence on information systems makes the information infrastructure vulnerable to information attacks. The defence and intelligence agencies are heavily dependent on commercial information infrastructure. It is not only that governments lack the resources and means to handle the plethora of information and have turned to commercial providers, but also that in certain cases (like satellite intelligence), the same information can be accessed by various users. The free flow of classified technologies and expertise to the private sector on the one hand and the use of commercial off-the-shelf technologies and expertise by the intelligence community on the other hand, seem to blur the boundaries between the national and commercial use of intelligence. [7] The fact that governments have lost the monopoly in the area of Information Technology means that they can not control the pace of technological developments in the commercial sector and thereby sophisticated Information Technology can be utilized by anyone. Adding to the above, since intelligence agencies are not the sole providers of information, they have to compete with academic institutions, think-tanks and private organizations.

The changes brought about by the Information Revolution exceed the hardware and software and also affects the organization and culture of the intelligence community. The modern intelligence community that evolved during the Cold War has acquired all the characteristics of large Weberian bureaucracies. [8] The intelligence agencies that emerged from the Cold War were hierarchical, stove-piped, secretive and resembled ‘information industries’. This model has proven inflexible and ineffective in the post Cold War era. The information and communication technologies call for the adoption of flatter, networked and task-oriented structures. Horizontal knowledge networks undermine existing structures that privilege compartmentalization, vertical integration, and classification. [9]

Finally, Information Technology has also altered the way intelligence consumers interact with information. In the recent past, information was scarce (often the product of clandestine operations), expensive and considered authoritative. On the contrary, information nowadays is relatively accessible, cheap and more tangible. As a result, intelligence consumers tend to function as their own analysts. They collect and evaluate information themselves and are reluctant to accept wisdom from authority. [10]

2. 2 The 'Open Source Intelligence' Promise

One of the most important developments in the field of intelligence is the qualitative improvements and volume growth in Open Source Intelligence/Information. Open Source Intelligence is a relatively cost-effective way of taking full advantage of the available expertise in any area of concern and due to its non-restrictive nature can be easily tailored and disseminated. OSINT makes up 70-80 percent of the intelligence data base. [11]

Robert Steele, a widely recognised advocate, argues that intelligence in the Information Age needs to be reinvented on the basis of Open Source Intelligence. OSINT is more than just information and can be much more than a valuable contributor to all-source intelligence. Open sources and cooperation with non-governmental sources of information point away from a small group of secret government bureaucracies and toward a virtual intelligence community. If properly integrated in national intelligence, OSINT can serve as an intelligence multiplier and cost saver and transform the intelligence process. [12] Stephen Mercado, a CIA analyst, praises the importance of OSINT and argues that OSINT should be treated as seriously as the other traditional sources of intelligence (imagery, signals, human etc) and even brings up for discussion the creation of a national OSINT centre. [13] A central issue regarding the utilisation of OSINT is whether the latter should be developed mainly in the private sector or incorporated within the national intelligence system. [14] In both cases OSINT has to overcome bureaucratic obstacles, fight for its share of the budget and also outfight institutional rivalries deriving from the other well established and already institutionalised intelligence disciplines (Signal Intelligence, Imagery Intelligence etc).

However, OSINT has also its limitations. Information overload, the spread of unreliable information and disinformation by media sources, as well as the security implications of privatizing parts of the intelligence production are among these limitations. In particular, one of the major disadvantages that Information Revolution brings about is information overload. The drawback of OSINT is that it threatens to weigh down the intelligence process and diminish the gains from technical improvements in intelligence collection and dissemination. Intelligence agencies are struggling to overcome this problem by turning to the private sector. [15] Although the private sector companies may assist in sorting out and *characterising* (putting in context) an immense amount of raw data, they may not be equally successful in

discerning between information and disinformation. As the amount of available information (and misinformation) continues to increase, isolating information with intelligence value that is relevant, timely, and accurate may become even more difficult. The spread of unreliable information is not a new issue, but due to the growth of media sources and the global reach of the Web, the amount of disinformation and propaganda has inevitable been increased. [16]

The ‘privatization of intelligence’, entrusting part of the intelligence process to the private sector is another point of criticism. Outsourcing certain ‘non-core’ functions would perhaps enable intelligence analysts to spend more time mastering the ‘core functions’, their core competencies. [17] Nevertheless, OSINT provided by the private sector varies tremendously in quality and reliability. OSINT is primarily driven by commercial considerations and thereby tends to focus on aspects which may be ephemeral rather than fundamental. Underlying trends or subjects, vital to national intelligence planning, that are considered to be too technical or arcane are less likely to merit commercial attention and investment. [18]

The intelligence community and corporations have similarities in the way they operate, but they have also profound differences. William Lahneman identifies two critical ones. [19] First, corporations struggle to maximize profit, while the intelligence agencies seek to maximize performance (identifying threats, early warning etc). Therefore, corporations can adopt policies that deliberately permit a certain percentage of failures. For example, if a failure is defined as an unfilled order, a company might maximize profit by allowing a certain percentage of orders to go unfilled as this policy lowers inventory costs. This is obviously not an option for the intelligence community. Intelligence agencies try to achieve a ‘zero defects’ performance record, since a defect could lead to an intelligence failure, which is clearly unacceptable.

Second, businesses have the option to exit markets in which they have become non-competitive, and enter some new market where they might achieve greater profitability. The same does not apply in the intelligence agencies. There is no intelligence agency that can simply neglect one issue of national security and focus on another, simply because the production of intelligence on the latter is an easier or more productive task. [20]

Apart from the above, intelligence from the private sector is available to almost anyone and therefore the number of potential threats can be increased. Bearing in

mind the developments in satellite technology, commercial imagery can be provided to a number of actors, including rogue states and terrorist groups. [21] It is possible, that less technical-developed nations or terrorist groups that are unable to conduct massive technical research will take the shortcut and turn to open sources.

Finally and despite its utility, OSINT may not be able to surpass preconceptions and tendencies, which are inherent in the culture of intelligence. Intelligence consumers (policy-makers) usually want to receive information unavailable from their own reading or viewing of the media. They want intelligence from secret agents and technical sources. There is also the danger that analysts might *spice up* their product, in order to add something 'secret' and gain the attention of their consumers. [22]

2. 3 Openness and the culture of secrecy

The above developments are inarguably important in shaping intelligence in the twenty-first century, but there is one element that has been neglected, the place of intelligence in society. Intelligence services have to be accountable, open, and function in ways compatible with the cultural norms, tradition and laws that characterize the information society. The emergence of a post-modern society and the challenges of globalization have made the world more complex, interdependent and dominated by risk. [23] The twentieth century has been described as the 'secret intelligence' era, where the primary goal was the protection and stealing of secrets. Although that remains one of the primary missions of intelligence, both the means of collecting part of the necessary intelligence and the (western) societies within which intelligence operates have been transformed. Becoming more open or remaining secretive is an important dilemma for intelligence services operating in democracies. [24]

Secrecy is after all a virtue and a necessity in the practice of intelligence. The sources of information and the methods by which information is gathered must remain unknown to the targets of intelligence. But at the same time intelligence services require public support and need to earn public trust. Without such support and trust, the services will lack legitimacy and credibility and their judgments will be questioned by the intelligence consumers, the policymakers. Advocates of openness argue that declassification and greater transparency will 'rationalise' certain operations (clandestine operations) in the eyes of the public and even counter the enemy's propaganda since the information released by the intelligence services will

offer their side of the story and influence the public and world opinion. [25] Critics of the openness argument contrast the difficulties, costs and risks in revealing secrets and claim that despite its problems the 'culture of secrecy' has served the intelligence community well. [26]

Wesley Wark takes the openness argument a step further and argues that the twenty-first century may prove the age of 'public intelligence'. For example both Britain and the United States, felt compelled in the aftermath of 9/11 to *publicize* some of their intelligence, to offer evidence and arguments in support of decisions on war. The release by the British government of the Joint Intelligence Committee assessment of the threat posed by Iraq's WMD Programmes in September 2002, the release of a declassified version of the CIA's National Intelligence Estimate (NIE) on Iraq's WMD on October 2002 and the televised presentation made to the UN Security Council by Secretary of State Colin Powell in February 2003, all reflected the need to rationalise in both ethical and legal terms the decision to declare war. [27]

The use of intelligence in the public domain in order to influence domestic and global public opinion is a crucial, but also controversial element. Before the decision to invade Iraq, speeches given by senior officers did not describe in detail the disparate sources or the complex analytical reasoning that lay behind the intelligence judgments that were cited. Some observers believe that intelligence was simplified to the point of distortion in order to shape the public debate. Others defend the use of accurate, if summarized, intelligence judgements on issues such as Iraqi WMD efforts and ties to terrorists, noting that full disclosure of analytical caveats is impossible. The implications of the above in the practice of intelligence are profound. Providing intelligence for public consumption requires different criteria and methods than intelligence delivered to traditional consumers. [28] In the end, supporters of a more transparent and accountable intelligence system have to take under consideration the benefits that the culture of secrecy brings in the practice of intelligence, and make sure that openness will not have a boomerang effect.

3. Challenging the Revolutionary Argument in Intelligence Affairs

Truly, Information Revolution has changed the way intelligence functions. The means of collection and dissemination have been transformed and new organizational principles are being applied. The conflict spectrum that intelligence officers have to

cover has been broadened and the expectations by both the public and the policy makers have been raised. Nevertheless, suggesting that all the above changes simply constitute a revolution in intelligence affairs is premature. There are certain issues that should be taken under consideration in any effort to revolutionize the intelligence process. These issues are not only principles, truths that are inherent in the practice of intelligence and its pathology and will inevitably appear in any new-alternative intelligence model, but also case specific ones that are related to the application of an IT-driven and network oriented alternative model in intelligence affairs.

3.1 Intelligence Failure

It is fair to argue that failure is an inevitable aspect of any human activity and thereby intelligence failure is an inescapable truth that everybody in the intelligence community has to live with. [29] This is not to 'rationalize' intelligence failure or to claim that no revolutionary approach or reform can reduce the possibilities of strategic surprise, but rather not to raise any unreasonable expectations of what intelligence can offer. In the best case scenario, the utilization of information technology, open source information and alternative methods of analysis, will clear some of the *fog* and the *noise* that is inherent in the intelligence practice, but will not prevent all the cases of surprise and failure. Preconceptions, ethno-centrism, mirror-imaging, group-thinking, politicization, luck and a culture of secrecy are always in play.

3.2 Politicization of Intelligence

Intelligence analysis must take policy needs into consideration in order to be relevant and useful. There is a fine line between being relevant and being overly supportive. When analysts are taking a purely neutral stance toward the existing policy (independent objectivity), the intelligence estimates are largely ignored by the policy-makers. When on the other hand, analysts are providing dangerously inaccurate intelligence in order to support a certain policy, then intelligence is actually jeopardizing not only its credibility, but also the national security policy. No reform, however drastic will overcome this paradox. In contrast to the traditional model, which limited interaction between intelligence producers and consumers, in order to ensure objectivity and avoid politicization, the alternative model aims to bring the analyst closer to the consumer in order to gain flexibility. Reformers and in extension

intelligence analysts and consumers must be aware of this limitation and balance between flexibility and politicization.

3.3 Information Technology is just a tool

The importance of Information Technology should not be overstated. Technology has always affected intelligence (Signal Intelligence, Imagery Intelligence), but has never transformed the nature of intelligence. Technology can be a powerful tool to overcome secrets and penetrate what is hidden, but it might also complicate the practice of intelligence by increasing the volume of available information and raise security concerns due to its dependence on technological means. Technology will always be a driver of change, but not the only one. [30] Apart from technology, there must also be a willingness to consider and adopt new operational and organisational changes that require increased transparency, improved training and better coordination. For example sharing intelligence rapidly across many agencies was difficult until the recent past, due to technological constraints. Although these constraints have been surpassed nowadays, the notion of 'data ownership' still exists. Achieving a real all-source analysis is not only a matter of technology, but mainly a matter of culture.

3.4 Information Overload

More information/intelligence does not mean better information/intelligence. More information might actually produce more disinformation and propaganda. Information overload was always a problem for intelligence systems, but what has changed from the recent past is the sheer volume of both signals and noise. As the mass of raw intelligence grows, it spawns worrisome problems for intelligence warning, analytical failures, and politicisation and manipulation of data and assessments by decision-makers. Open source information and widely interconnected networks have a lot to offer in every stage of the intelligence cycle, but unless the information is properly managed and coordinated, the system might fail. The traditional intelligence model, which was characterized by centralized planning, a hierarchical chain of command and formal procedures failed to deal successfully with information overload. Whether fluid and decentralized networks are the proper organizational paradigm to ensure adequate accountability and prevent incidents of micro and macro-management of information, as its proponents claim, deserves closer attention. [31]

3.5 If it works in the Business Sector, it will also work in the IC

It is true that certain lessons from the business sector can be applied in the intelligence sector (virtual corporation, information sharing, flat structures and knowledge management). [32] For example, the business sector appears to be significantly ahead of government in acting to reduce stovepiping, and can serve as a valuable resource for the intelligence community. [33] But there are also great differences between the two communities. The business sector defines cost and profit in a different manner than is the case in the intelligence *industry* and the latter can not simply shift its priorities to a new profitable area. In the business sector the information flows freely through the networks. In the intelligence sector, very often networks are destroyed, information flows are discontinued and sensors are deceived. In the business world, information networks compete, whereas in the military world, they might also be destroyed. As a result, information superiority in the market does not necessary translate into information superiority in the intelligence community.

3.6 Outsourcing of Intelligence

Entrusting part of the intelligence production to private organization, has both advantages and disadvantages. Intelligence provided by the private sector is important in order to manage information overload and provide timely and sound intelligence. On the other hand, the quality of the intelligence produced might vary. The private sector might be unaware (for reasons that have to do with national security) or unable to understand, what an intelligence consumer is looking for. In addition the private sector is concentrating on providing short term analysis and not long term assessments. Furthermore, Open Source Intelligence abolishes the monopoly that intelligence agencies had in the ‘knowledge’ industry. Whether this atypical form of antagonism will benefit the intelligence services or whether the latter will fight turf wars to defend their preferential status or even their existence, is hard to say for the time being.

3.7 The Producer-Consumer Relationship

The fact that policy-makers have the ability to select and download material from the same raw and finished intelligence product that is available to the intelligence analyst, has major implications for the producer-consumer relationship. This new pull architecture should theoretically improve the ability of consumers to identify the

necessary material and have access to more than one view. In this process, decision-makers initially tend to bypass middle-level managers and access the data on their own or speak directly with the field specialist. This tendency reinforces the development of flatter management structures. One major risk of the new pull architecture is that consumers with direct access to a comprehensive intelligence database may take it upon themselves to act as their own intelligence analysts, either through hubris, dissatisfaction with the existing service or because of time constraints. [34]

4. Conclusions

To conclude, a paradigm shift in intelligence affairs has not occurred. The Intelligence Community is just starting to adapt to the technological, organizational and cultural challenges that Information Revolution brings about. Revolutionary enthusiasts have to come to terms with the nature of Intelligence. Failure and politicization are inherent in the nature of intelligence and ambitious proposals will at best minimize such effects. Outsourcing intelligence and open source information seem to be double-edged sword and reformers must be careful not to jeopardize the product of intelligence or create unreasonable expectations for the public and the policy-makers. Finally, attention should also be devoted to the most important asset, the human element and the need to balance between the art and science of analysis, between human instincts and scientific judgments.

Strictly speaking, intelligence is in a phase of transition, but it is too early to conclude whether this transition will result in a revolution or will end up being just an evolutionary development. The conflict spectrum is widened compared to the traditional Cold War threats and the mission of intelligence in the uncertain international environment is definitely broadened, but not transformed. New technological assets have been added to the analyst’s toolkit and new organizational concepts have been applied in the intelligence cycle, but the craft of intelligence remains fundamentally the same. Redefining the role of intelligence, readdressing the relationship between analysts and consumers, making the best of open source information, using alternative methods of analysis, managing information overload, making intelligence available to the public and minimizing politicization, are some of the challenges that intelligence is facing in the twenty-first century. Although some of

the above are not new, they still pose great risk to the practice of intelligence and by extension to national and international security.

Any effort to reform the intelligence community, to apply a revolutionary model has to take under serious consideration various aspects. Information Revolution has redefined the way in which intelligence is used and conceived. The old demarcation lines between and intelligence and information, operations and intelligence, consumers and providers, national and private intelligence has become blurred. Change, of a revolutionary magnitude or not, requires more than just rewiring the organizational charts of the Intelligence Community. Any effort to reform intelligence must adopt a holistic approach and not rely solely on the advantages that information and communication technologies bring about. In sharp contrast to what politicians and reformers with a political agenda believe, such an effort will require significant time to come to fruition and it can not be a quick fix. The decision to reform the community might be revolutionary, but the implementation is always incremental.

Notes

[1] See Andrew Rathmell, 'Towards Postmodern Intelligence', *Intelligence and National Security*, 17, 3 (2002) and Wesley K. Wark, 'Introduction: Learning to Live With Intelligence', *Intelligence and National Security*, 18, 4 (2003).

[2] See Robert D. Steele, *On Intelligence. Spies and Secrecy in an Open World* (Fairfax Virginia: AFCEA International Press, 2000) and Bruce D. Berkowitz and Alan E. Goodman, *Best Truth. Intelligence in the Information Age* (New Haven: Yale University Press, 2000).

[3] For a selected list of works about the challenges that the Intelligence Community is facing in the early twenty-first century see selectively Harold Shukman (ed.), *Agents for Change. Intelligence Services in the Twenty-First Century* (London: St' Ermins Press, 2000), Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information* (Cambridge: Cambridge University Press, 2001) and Wesley Wark (ed.), *Twenty-First Century Intelligence* (London: Frank Cass, 2004).

[4] Bruce D. Berkowitz, 'Information Technology and Intelligence Reform', *Orbis*, (1997), pp.109-111.

[5] Berkowitz and Goodman, *Best Truth*, pp.17-18.

[6] Sharfman, Peter, 'Intelligence Analysis in an Age of Electronic Dissemination' in Charters, David et.al, *Intelligence Analysis and Assessment* (London: Frank Cass, 1996), pp.201-203.

[7] Rathmell, 'Towards Postmodern Intelligence', p.98.

[8] Michael Herman, *Intelligence. Power in Peace and War* (Cambridge: Cambridge University Press, 1999), p.324.

[9] Rathmell, 'Towards Postmodern Intelligence', p.91, 99.

[10] Berkowitz and Goodman, *Best Truth*, pp.21-22.

[11] Alan Dupont, 'Intelligence for the Twenty-First Century', *Intelligence and National Security*, 18, 4 (2003), p.26. Hulnick characterizes it as the *lifeblood of intelligence* and argues that considering the increased information flow in the post Cold War era, including that from closed societies, that estimate may be too low Arthur S. Hulnick, 'The Downside of Open Source Intelligence' *International Journal of Intelligence and Counterintelligence*, 15, 4 (2002), p.566.

[12] Steele, *On Intelligence*, pp.105-126.

[13] Stephen C. Mercado, 'Sailing the Sea of OSINT in the Information Age', *CIA Studies in Intelligence*, 48, 3 (2004) and Stephen C. Mercado, 'Reexamining the Distinction Between Open Information and Secrets', *CIA Studies in Intelligence*, 49, 2 (2005).

[14] Stevyn Gibson, 'Open Source Intelligence. An Intelligence Lifeline', *RUSI Journal* (February 2004), p.20.
[15] For example, the Central Intelligence Agency (CIA) has set up a non-profit, venture capital company called IN-Q-TEL, which develops techniques to sort, order, and deliver raw intelligence so that analysts are not overwhelmed by the enormous amount of information. Rick E., Yannuzzi, 'In-Q-Tel: A New Partnership Between the CIA and the Private Sector', *Defence Intelligence Journal*, 9, 1 (2000), pp.25-38.
[16] Hulnick, 'The Downside of Open Source Intelligence', pp.567-568.
[17] William J. Lahneman, 'Outsourcing the IC's Stovepipes?', *International Journal of Intelligence and Counterintelligence*, 16, 4 (2003), pp.573-593.
[18] Dupont, 'Intelligence for the Twenty-First Century', p.28.
[19] Lahneman, 'Outsourcing the IC's Stovepipes?', pp.575-576.
[20] Ibid.
[21] Dupont, 'Intelligence for the Twenty-First Century', p.27.
[22] Hulnick, 'The Downside of Open Source Intelligence', p.573.
[23] Beck Ulrich, *Wold Risk Society* (Cambridge: Polity Press, 2001).
[24] For a detailed analysis of this dilemma see selectively Arthur S. Hulnick, 'Openness: Being Public about Secret Intelligence' *International Journal of Intelligence and Counterintelligence*, 12, 4 (1999), pp.463-483 and Thomas Patrick Carroll, 'The Case Against Intelligence Openness' *International Journal of Intelligence and Counterintelligence*, 14, 4 (2001), pp.559-574.
[25] Hulnick, 'Openness: Being Public about Secret Intelligence'.
[26] Carroll, 'The Case Against Intelligence Openness'.
[27] Wark, 'Introduction: Learning to Live With Intelligence', pp.8-9.
[28] Ibid.
[29] See Michael A. Turner, *Why Secret Intelligence Fails* (Washington DC: Brassey's Inc, 2005).
[30] Wark, 'Introduction: Learning to Live With Intelligence', pp.3-4.
[31] Berkowitz and Goodman, *Best Truth*, pp.92-93.
[32] Edward Waltz, *Knowledge Management in the Intelligence Enterprise* (Boston: Artech House, 2003).
[33] Lahneman, 'Outsourcing the IC's Stovepipes?', p.589.
[34] Dupont, 'Intelligence for the Twenty-First Century', p.24.

About the Author

Dr. Andrew Liaropoulos is a Research Associate in the *Callaghan Centre for the Study of Conflict* and a member of the Administrative Board of the *Research Institute for European and American Studies*. His research interests are Security, Intelligence and Military Transformation.

RIEAS RESEARCH PAPERS

Andrea K. Riemer, (2006), "Geopolitics of Oil: Strategic and Operative Causes for the Iraq Intervention", RIEAS: Research Paper. No.99, (February).

Andrea K. Riemer, (2005), "Nation Building: Concepts, Definitions, Strategic Challenges and Options", RIEAS: Research Paper. No.98, (November).

Pine Roehrs, (2005), "Weak States and Implications for Regional Security: A Case Study of Georgian Instability and Caspian Regional Insecurity", RIEAS: Research Paper, No. 97, (October).

Vassiliki N. Koutrakou, (2005), "Insights into the Post 2000 WTO- Inspired Development Policies Sponsored by the G 8 and the European Union", RIEAS: Research Paper, No.96, (June).

Andrea K. Riemer, (2005), "The Kurds: Between Ankara and Baghdad in Search of Independence", RIEAS: Research Paper, No. 95, (May).

Yannis A. Stivachtis, (2005), "The European Security and Defense Policy (ESDP): Evolution and Challenges", RIEAS: Research Paper, No. 94, (March).

Andrea K. Riemer, (2004), "Turkey: In a European-U.S. Crunch?" RIEAS: Research Paper, No.93, (November).

John M. Nomikos, (2004), "European Union Intelligence Service: A Necessary Institution for Confronting Terrorism?" RIEAS: Research Paper, No.92, (April).

Vincent Wei-cheng Wang, (2003), "The New Dawn of Strategic Asia: U.S. Policy Toward the Asia-Pacific Since September 11", RIEAS: Research Paper, No. 91, (October).

Alain Faupin, (2003), "Reform of the French Intelligence Services After the End of the Cold War", RIEAS: Research Paper, No. 90, (March).