CROSS-DOMAIN APPROACHES TO INTELLIGENCE ANALYSIS

Daniela Bacheș[i]-Torres
Efren R. Torres[ii]-Bacheș

> *"Understanding the needs of the consumer and the sources available enable an analyst to choose the correct methodology to arrive at useful answers."*
>
> (- James A. Williams, LTG, U.S. Army (Ret.)
> Former Director, Defense Intelligence Agency)

Introduction

Twenty-first century decision-making has reached the need of all-source intelligence knowledge, which requires the transfer of information between different domains. Concurrently, intelligence has evolved from being the prerogative of the Government to an instrument in the hands of the private sector, academia and even international organizations, agencies and NGOs[1] that turned into concomitant consumers and producers of situational awareness in real-time. These changes have led to new requirements in the intelligence analysis tradecraft that involve integration of ideas, backgrounds and perspectives, together with expertise and experience sharing to enable creative, innovative and efficient answers to present and future questions. Fundamentally, the model of cross-domain collaboration in the sciences has translated to the Intelligence

[i] Daniela Bacheș-Torres is a PhD Candidate at Brunel University, UK. Email: elena.baches@brunel.ac.uk.

[ii] Efren R. Torres-Bacheș is an intelligence analyst working in the private sector. Email: efren.r.torres@gmail.com

Community[iii] (IC) as a prerequisite for the success of the intelligence enterprise.[2] Thus, bringing together multi-sector insights is the first step in identifying common grounds for a cross-domain collaborative debate that can contribute to the development of efficient tools and methods adapted to the transformation of intelligence analysis.

In a world where the understanding of threats and risks has become a complex challenge, analysts are required to produce actionable intelligence needed to strengthen *a priori* collective resilience in the face of tomorrow's unknown(s). In order to protect their respective homelands and interests domestically and overseas, governments need to provide accurate and timely analyses not only to inform policy-makers, but also to support and enhance intelligence-led capacity-building for prevention, intervention and enforcement action.

Similar to governments, the private sector also has the mission and the need to protect company assets at the domestic and at the international level. Within this past decade, the private sector has created intelligence units in order to rely less on government-generated intelligence and more on the in-house production of information. Private Sector Intelligence (PSI)[3] is tailored to address the existing threats affecting a company's respective industry in order to prevent surprises that may have an impact on business operations and safety.

The professionalization of intelligence in the private sector and the emergence of a multi-faceted private intelligence community has been discussed by Robert M. Clark, who looked at how

> "(...) globalization and the increasing need for government, NGOs, and commercial firms to acquire information across the globe has fueled an industry. Today many firms provide worldwide open source information forming what has been called a "private-sector intelligence community". (...) In addition, many firms provide very specialized open source information tailored to commercial firms in sectors such as banking, agriculture, and energy".[4]

Clark's assessment refers to the emergence of a hybrid phenomenon engaging (with) both the private and the government sector: the privatization of Intelligence and the emergence of the Intelligence-contracting industry. Since the late 1990s, both government agencies and corporations have outsourced analytic and operational work to companies that provide general, scientific or technological intelligence[iv] products. While for Governments the outsourcing of intelligence is mainly due to a reduction of costs and increase of efficiency of the IC activities[5], the industries' use of commercial intelligence is determined by the need to secure

[iii] The Intelligence Community has a broad meaning here, referring to the various communities of practice in Intelligence (both government and private, national or international).

[iv] The classification is taken from the website of the Australian Department of Defense. Available at http://www.defence.gov.au/dio/what-we-do.shtml.

operations and assets in contexts of risk.

Parallel to the national intelligence tradecraft, in 1973, three Yale professors were emphasizing the emergence of Intelligence activities that bureaucratic structures of the major international organizations were engaging in. In their case, the intelligence tradecraft was made of "complex osmotic strands, which frequently prove extremely effective despite their low level of visibility."[6] Forty years later, international organizations continue to develop intelligence capabilities to support their activities, facilitate the achievement of their goals and enable the implementation of their functions[7]. The United Nations has developed intelligence capabilities in support of the peace operations; the analytic products it has elaborated constructed the basis for enhanced mission planning and decision making[8]. Intelligence analysis is a multilateral process based on the acquisition and integration of "information from all mission components and other sources, in order to develop analytical products that are timely, accurate, complete and usable[9]". At the same time, the added value provided by the analytic products issued by international entities contribute to strengthening organizational leadership and legitimacy, while supporting the decision making process. An interesting example is the European Union (EU) which has developed its own strategic analysis capacity; the work conducted daily by analysts of the Intelligence Centre (INTCEN) is aimed at providing guidance for timely and coordinated response to major crises.

The 21st century has witnessed the empowerment of non-governmental intelligence as a result of increased sophistication and power open-source tools and infrastructure for data and information gathering:

> "In December 2002 the Institute for Science and International Security (ISIS), a Washington-based non-governmental organization, announced that it had found two previously undisclosed nuclear facilities in Iran. Using information provided by a dissident group called the National Council of Resistance of Iran (NCRI), ISIS was able to pinpoint the two suspect sites by using general geographic descriptions provided by NCRI to find more precise mapping coordinates".[10]

The emergence of non-governmental organizations (NGOs) as important players in international affairs enabled the development of intelligence capabilities they needed to conduct their activities. Thus, as NGO employees are often already present in remote regions, they have access to local information that governments might never reach due to various reasons, from cultural and diplomatic disputes to financial aspects. Consequently, this created an intelligence capital of interest to states that led to the establishment of intelligence-sharing between NGOs and governments[11].

Academia has been an important contributor to the consolidation of NGO-driven intelligence and analytic capabilities. As emphasized above, NGOs have access to a wide range of sources that are able to provide them with "situational awareness and an understanding of the threat environment"[12]. As in the case of international organizations, the intelligence capitalization process is tacit and latent, which allows them to integrate social science research methods in the elaboration of their analytic products. What academic methods and studies in many of the social sciences may provide is basis for intelligence analysis[13] - whether it is conducted by NGOs, in particular, by any other entity producing intelligence. By helping shape the strategic context, scholars and Subject Matter Experts (SMEs) provide knowledge that acts as complementary expertise to the analyst's understanding of the general picture.

Whether we consider the governmental or non-governmental sectors, the public or the private intelligence tradecraft, the profit or non-profit fields, intelligence production serves the improvement of each entity's security, and aims at contributing to the achievement of established goals mainly by avoiding unwanted surprises. But while procedures are rather similar, the tools and resources used may know significant variations that are specific to each domain. In many cases, this situation translates into the 'self-standing' of these communities of practice, which leads to the isolation of practitioners and best practices. Consequently, both on theoretical and practical grounds, cross-domain interaction becomes a must for more efficiency in the goal-reaching process of intelligence analysis.

Cross-domain approaches: setting-up a dialogue

A *cross-domain approach* brings together best practices, standards, methods and instruments from different fields of practice to provide an all-inclusive understanding of one process that knows multiple representations and methodologies. The concept builds on a series of key features characteristic of various spheres of activity and practice; when associated to an autonomous process, these features can lead to a comprehensive implementation able to create efficient solutions to complex problems through a 360-degree view.

In comparison to cross-disciplinarity, which refers rather to activities that involve aspects from various academic disciplines, a cross-domain approach integrates, besides the knowledge capital achieved through the gathering of expertise, applied techniques and know-how rooted in multiple cultures of practice. Moreover, a cross-domain approach not only bridges different sectors and actors, but it also reaches across boundaries of expertise that are many times decisive in finings (joint) solutions to security puzzles.

The cross-domain approach was first used in the Army as an expression of the combination of different capabilities (land, sea, air, space and cyberspace) coming from various military services to achieve joint power. The need of a cross-domain synergy is emerging in the face of a "future of complex challenges and constrained resources[14]" which requires not just the interaction and cooperation between various entities putting together the same set of capabilities, but rather different yet complementary capabilities. Consequently, in addition to creating an integrated product greater than the sum of separate outcomes that entities could reach independently, the cross-domain approach extends the effect from a specific result, achieved in a well-determined context, to the improvement of operational performace *per se.*

Moreover, the creation of multi-domain perspectives equates to the building up of a more comprehensive view[15] of the self, of the other (friend or foe) and of the environment. As a result, the broadening of intelligence analysis through the cross-domain perspective on the enemies becomes a 'must', given the 360-degree view potential of such an approach to identify and understand their motivations, critical vulnerabilities, centre of gravity, intentions and actions[16]. However, it must be underlined that while such an approach has represented a great achievement in building-up efficient solutions for the future, it remains limited to the culture of the same community or sector of practice: the Army. For this reason, whether one looks at collaboration between the various departments of one organization, the various organizations of a large community of practice, or even the entities accomplishing different functions within a more or less formal or institutionalized context, all the actors involved share a set of functioning patterns that make them tributary to similar mindsets in the organization and operationalization of knowledge.

The purpose of this issue is to engage the wide audience of scholars, practitioners and experts across various domains, sectors and fields of practice in a constructive discussion about intelligence analysis. The mission of this issue is two-fold.

The first and main goal is to raise awareness that intelligence analysis is a practice that is branching out of government agencies into new industries. For decades, intelligence in the private sector has been seen as a business tool that generates revenue for a company. However, as companies have started to take action to mitigate new emerging threats, they have taken steps necessary to recruit former members of the IC to create their own intelligence units; these units are responsible for assessing threats and providing the company with early warnings of possible risks relevant to their industry. This is just one example of how intelligence has gained independence from its birth parents, government agencies and the military.

The second goal is to unite all parties: academia, government, military and private sector in order to provide insightful perspectives on intelligence analysis (issues, methodology and practice) from all possible angles of practice and studies. Only by communicating and discussing about the different sectors in which intelligence analysis can be applied, can practices improve and the intelligence literature grow and expand through newly established research agendas. In addition, by increasing awareness on the expansion of the analytic tradecraft, intelligence analysts from all public and private industries and sectors can create and join “analysis networks and working groups to share their own best practices and lessons learned with each other”[17]. Such a collective initiative has the potential to leverage analytic expertise for better addressing security needs and challenges.

Literature Gaps: What is Literature (not) Telling Us ?

Despite the various issues in intelligence analysis discussed in the literature, the challenges that intelligence analysts face -to keep pace with newest developments in technical skills and evolving threats- has been little addressed so far.

While intelligence analysis has established itself as a practice outside the Government sector, most of the scholars have manifested domain dependence[v], failing to acknowledge the emergence of a community of intelligence practitioners in the private industry, as well as the civil society[18], academia, R&D or international organizations. Thus, intelligence as a discipline has always seemed only relevant when applied to the Government, in spite of the fact that the intelligence tradecraft has been applied as early as 1500 B.C. by Phoenician traders seeking to expand their maritime empire.[19] In addition, ICs across the world are still holding onto Cold War mindsets by only considering that information significant/relevant to national security comes from secret sources and can only be assessed within and for national governments. As a result, much of the open-source knowledge and expertise existing outside the borders of the IC is being neglected. In other words, there is an ignored capital of intelligence in academia and think thanks, private companies and scientific research centers, non-governmental organizations and international bodies that remains stuck within the walls of each domain and insufficiently exploited due to a lack of communication between and across fields of practice.

A first category of initiatives trying to address the analytic process from a different perspective looks at the relation between analysts and decision-makers in the context of the intelligence cycle. Both scholars and practitioners writing on this topic have been interested in understanding the intelligence-policy relation and the possible ways to reduce the cultural gap between producers and customers, and therefore increase the value of the analytic product for the decision-making process. Back in 2007, Barry et. al made the case of accepting that “intelligence and policy personnel have to function as members of a team, and that direct communication, feedback, and careful tailoring of support are essential”.[20]

Another interesting approach was developed by Stephen Marrin who argues for exploring inter-disciplinary connections that would enable intelligence analysis to improve its best practices[21]. However, whereas Marrin’s contribution opens

[v] The concept of ‘domain dependence’ has been introduced by Nassim Nicholas Taleb in his book *Antifragile: Things That Gain from Disorder*. New York: Random House. 2012.

new valuable perspectives both for the future development of an intelligence (analysis) theory, as well as the practitioners' work, his definition of intelligence analysis remains tributary to the Government's efforts to maintain national security. At the same time, most of the contributions gathered by Marrin in the 32nd Volume of the *Intelligence and National Security (INS)* Journal[22] remain devoted to an academic perspective and how the social sciences methodologies and concepts can contribute to improve the traditional IC analytic tradecraft.

A similar endeavor meant to provide a broader and comprehensive understanding of the analytic process is the collective volume published by the National Research Council on *Intelligence Analysis: Behavioral and Social Scientific Foundations*[23]. The volume gathers contributions meant to provide scientific guidance to the analytic process (namely three specific aspects: analytic methods, analysts and organizations) through the lenses of different approaches from social sciences. Although the book does not build an integrated perspective on the overall analytic process, the various contributors give the opportunity to the reader to get a better understanding of the various components and micro-processes embodied in the intelligence analysis practice.

Thomas Finger's first chapter makes a strong point on the plurality of the IC in terms of its members' missions, customers, professional identities, and organizational cultures[24]. Even though each agency is meant to pull up its resources and staff to the overall goal of enhancing national security, diversity of problems and customers (both individual and institutional), division of analytic labor and field specialization (political, economic, societal, etc) determine a pluralistic arrangement of the IC both in terms of structure and functions. Consequently, if this is the case within the national ICs, the emergence of new intelligence institutional players on the international scene, as a result of globalization and the increasingly complex security environment, lead to an even more obvious specialization of means and capabilities specific to each actor's needs and profile. Patrick F. Walsh describes this situation as the *fragmentation across intelligence communities,* a phenomenon that hindered knowledge transfer among practitioners in difference of intelligence[25]:

> "The relative siloing of intelligence into "policing", "national security" or "private sector" intelligence, has also produced a similar fragmentation of intelligence scholarship. Scholars tend to work in one field such as policing, rather than across one or more fields. This has also resulted in less cross-fertilization of ideas, knowledge and theory building within the broader intelligence field[26]."

Walsh's argument for bridging the gap across traditional and emerging practice areas has both a practical and a theoretical *raison-d'être*. On the one hand, the extension of intelligence networks gathering public and private specialized institutions is the inner result of the widening of the security agenda.[27] On the other hand, a better understanding of the "new age of intelligence"[28] is part of a broader initiative of deepening intelligence research and therefore contribute to the development of a discipline.

In another volume published by the National Research Council, *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*, the future of collaborative analysis includes integration of independent perspectives and expertise beyond the borders of the IC:

> "Intelligence in the age of global counterterrorism requires effective collaboration with groups both inside and outside the IC, including domestic and international agencies, private contractors, industry experts, and academics. These relationships can range from informal calls for advice to formal contracts".[29]

One of the fewest scholars who analyzed and made a valuable case for practitioners to collaborate with academics and use the intelligence literature in order to acquire new ways to think about, frame, conceptualize, and improve the analytic process and products[30] is Stephen Marrin. In his 2012 book on *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice[31],* Marrin advanced the practical utility of the dialogue between academia and practitioners. On the one hand, the results of intelligence research and scholarship developed within the academic environment can serve intelligence analysts throughout the various stages of their careers and support different needs of knowledge:

> "In order to successfully achieve their purpose, intelligence analysts need to process both subject matter knowledge related to their specific analytic focus (…), as well as process knowledge related to exactly how to do the work of analysis. To acquire subject matter knowledge useful for improving intelligence analysis, one might look to area studies, comparative politics, international relations, and other subject matter disciplines. But if one wants to acquire knowledge on the processes, concepts, and context for understanding and improving intelligence analysis, one would look to the intelligence studies literature".[32]

On the other hand, Marrin interestingly argues that the intelligence literature has an inner practical component, and therefore potential value for the intelligence tradecraft, as

> "the intelligence studies scholarship is much closer to practice than it is to theory. (…) the literature itself is generally applied in nature. The questions asked generally provide real-world, practitioner-oriented solutions".

Unfortunately, there is still a wide and clear gap in intelligence studies when it comes to addressing the role of traditional intelligence analysis applied to areas outside of the government context; the literature on private sector intelligence, for example, and the research on how these corporate intelligence units interact with the IC is non-existent.

As previously mentioned, the main goal of this issue is to raise awareness that intelligence analysis, as a practice, is evolving and adapting to new terrains such as the corporate world. Although there is a wealth of literature on business and competitive intelligence that date back to the 1950s, the exploration of how traditional intelligence can actually be applied to the private sector has been lacking; perhaps this highlights symptoms of disinterest and indifference by part of intelligence academics due to the misconception that if intelligence is applied to a business, it must be for the purpose of generating more profits.

In addition, this illness that academia is suffering from may be stemming from the fact that private sector intelligence units solely rely on open sources, thus, academics seem to believe that if intelligence does not deal with covert sources and secrets, it is not relevant or interesting enough to pursue as a topic of study. Issues such as politicization of intelligence, intelligence failures, and flawed communication with decision-makers, cognitive biases, espionage and ambiguity/unreliability of sources also deeply affect private sector intelligence units. Thus, it is very important that through this effort, academics and experts take the time to understand and scrutinize the information presented in this issue in order to fill the gaps of knowledge and develop the literature on intelligence analysis in the private sector.

Furthermore, despite the initiatives shown by the IC to engage with outside experts, as well as the increasing number of projects and initiatives in the private sector and academia[33] to support the development of the analytic tradecraft, a constructive dialogue, collaboration and joint engagement remain much limited. Moreover, exploring "ideas and alternative perspectives to gain insight, or generate new knowledge"[34] jointly is something extremely valuable; however, neither the community of practice nor academia has been willing so far to deeply commit to it. By exploring cross-domain perspective on intelligence analysis, the opinions gathered in this issue of the Journal of Mediterranean and Balkan Intelligence are trying to give a first glance on the value and importance of engaging a dialogue between scholars and analysts from different fields of practice (Government, private sector, non-governmental sector).

Exchanging Perspectives: Today's Look into Tomorrow's Becoming

The broader international IC (both public and private) is facing the challenge of having to mitigate new risks, and fight with complex foes that have been developing multiples sets of capabilities and skills by putting together knowledge, competences and expertise from a variety of fields and experts. This means that intelligence practitioners (analysts, managers, SMEs) are requested to adapt existing tools and methods, and to adopt new working processes to improve the analytic tradecraft in the image of the Future. Yet, History has proved many times that 'what has been will be again, what has been done will be done again; there is nothing new under the sun' (Ecclesiastes 1:9). In other words, Intelligence must both look into the known Past to protect the Future, and take aim to the changes of the Present.

Together with this Issue's contributors, we have tried to address some of the present-day practices, challenges and trends encountered in the field of intelligence analysis by bringing together the experience of and the research conducted by intelligence practitioners and scholars.

Gregory Treverton in his letter *The Future of Intelligence* provides this issue of the *Journal of Mediterranean and Balkan Intelligence* with an outlook of the challenges of intelligence during and after a Donald Trump era. Treverton cleverly asserts that intelligence is about storytelling, and intelligence failures occur when stories are not told in full. Moreover, Treverton makes reference to big data and the increasing importance of OSINT, especially through social media, which echoes throughout most contributions to this journal, but in particular, his ideas resonate in our closing article "*Experts' Look into the Future: 2027 Intelligence Analysis*" as these were common denominators among all of the contributions.

The RIS Open-Source Intelligence Cycle Article by Arno Reuser emphasizes what many academics and intelligence practitioners choose to disregard, the increasing role and importance of OSINT to the intelligence practice. Reuser makes a strong argument on why his proposed "propeller intelligence cycle" is more inclusive, time-efficient and overall a stronger model than those intelligence cycles currently existing in intelligence. Reuser's paper is high in value due to the fact that its content, his notion of a propeller intelligence cycle model, can be applied to both private companies and government in a very functional manner; however, issues with the availably of policymakers remain a challenge that will affect any future model of the intelligence cycle in any sector, public or private.

The original article written by Efren Torres on *Private Sector Intelligence Units (PSIUs),* details how conventional intelligence practices have adapted to serve private companies instead of being limited to serving the national policymaker. This article gives valuable insight on the difference between this traditional role of intelligence vs. competitive and business intelligence. Furthermore, this article serves as a catalyst for future new research by expanding the known intelligence studies literature and limited framework posed by academics by describing intelligence functions, organizational aspects as well as methods of PSIUs.

Jorhena Thomas in her article *Collection Planning. A Cross-Domain Approach* provides readers of intelligence with an in-depth explanation of cross-domain collection approaches. Moreover, Thomas acknowledges the importance of OSINT as a powerful tool in intelligence analysis. Thomas's paper addresses practitioners and academics by providing technical explanations and steps for the collection planning phase, which can be applied to the private sector and for national intelligence purposes.

Humberto Hinestrosa brings his valuable expertise from both the government and the private sector in his article on scenario analysis. In *Scenario Analysis: Combining Intelligence Analysis Method*, Hinestrosa explains the importance and the value that scenario building has for strategic intelligence. His article is very relevant to theme of this issue of the Journal of Mediterranean and Balkan Intelligence as it addresses a strategic tool that can be used by governments and private companies. Furthermore, he explains that in addition to provide strategic warning, scenarios are also a tool to improve communications between producers and consumers of intelligence, which is an issue that affects both the public and private sectors.

Aleksandra Bielska and Chris Pallaris's interesting work in *Addressing the Internal Challenges to Intelligence Work* touches on the very essence of the theme of this journal issue. While contributors discuss OSINT, private sector intelligence, competitive intelligence, history, etc., Bielska and Palaris share their experience and findings on what affects intelligence analysts and how to tackle these inefficiencies in the analytic process. Undoubtedly, issues with overtasking, excessive amounts of information and lack of IT training are very crucial factors that affect the quality of work done by analysts. This is very important knowledge for both academics and practitioners that could allow them to identify where the weak pillars are located and address them if (i) practices and quality of work are to be improved and (ii) if academics are to exit their comfort zone and explore other areas of intelligence that differ from old ongoing debates.

In *The Practice and Gap of Intelligence in Emerging Economies*, Juan Carlos Ladinez Azalia and William Castillo Stein bring the argument that the bridge between academia and practice is still an ideal even outside of the Anglosphere. Ladinez and Castillo bring an interesting and appreciated contribution to this journal given that it is rarely heard of intelligence studies from the perspective of Andean countries such as Peru. In their paper, they assert that intelligence in Peru is taboo and something that is not to be talked about in the open except as gossip. Overall, Ladinez and Castillo make the point that there is a growing interest in intelligence studies and academic engagement with policymakers in Peru, which could serve as the foundation for future research in intelligence outside of the Anglo-Saxon context.

Constant Hijzen's article titled *The History of Intelligence: Future Prospects* provides an awakening call to academics, experts and practitioners. Hijzen's argument that the historian of intelligence needs to learn to work closer with other academic colleagues from other domains is something that nobody has acknowledged. To this date, there is a lack of participation and inclusion of historians into current debates in intelligence, and Hijzen makes a good argument for the need to change it. Lastly, Hijzen does a very good job highlighting the value of historical knowledge for intelligence analysts.

The *National Strategic Intelligence and Competitive Intelligence* article by Avner Barnea gives this issue of the JMBI a fine contrast since it explains what competitive intelligence is and how it works. Furthermore, he draws parallels on how both practices (national intelligence and competitive intelligence) work in similar ways. The highlight of Barnea's paper is that it explains how competitive intelligence can help improve practices in national intelligence, and overall, emphasizes the benefits of having a partnership between private and public sectors.

The reflection papers provided by El Benni and Chopin & Oudet, help to fill in some of the gaps that have not been widely addressed in intelligence studies. In El Benni's reflection paper titled *Terrorist Intelligence Tradecraft: What the IC Should Know,* he addresses the importance for intelligence analysts to be widely aware of how terrorist networks collect and analyse intelligence. To this extent, the literature has not been very explicit. There have been discussions on modus operandi, but not in-depth analysis on how non-state actors have adopted intelligence practices drawn from national intelligence. Furthermore, Chopin and Oudet's article describe the little-known French intelligence community and the interaction with academia. This reflection paper makes the case to fix the lack of academic involvement and the need for scholars to be actively working with the French intelligence community.

Lastly, our closing article *Experts' Look into the Future: 2027 Intelligence Analysis* was aimed at providing the reader with a futuristic outlook on what intelligence analysis and security overall will be like in ten years and beyond. All the contributors addressed the same issues: the role of social media and problems with veracity/reliability of information available through open sources. The intention of this article was to lay the foundations for further discussions and debates on the role of intelligence in the upcoming decades. How will the new generation of analysts conduct intelligence analysis in both public and private sectors? Will OSINT become the predominant INT in the next decade? With the emergence of new technology, how will intelligence agencies be able to keep up with non-state actors that acquire said technology? All of these questions are worth considering as academics shape the debates in intelligence studies and security for the upcoming years.

Conclusions

Aside from intelligence analysts working within the IC, the analytic tradecraft is also being developed and improved on the daily basis by analysts working in other industries such as finance and business, entertainment, private security, operational research, hard science, engineering, statistics, economics and beyond. What all these analysts share in common is "the processing of data from one form to another, making sense of noisy or obscure concepts, working out what is true and what isn't, and communicating conclusions"[35] to decision-makers from various sectors.

Whether we refer to the government or the private sector IC, the proliferation of information has transformed the intelligence production, OSINT becoming the largest component of all entities' all-source intelligence capacity[36]. Thus, both as a strategic enabler for national security or a tactical driver for international military operations and corporate decision-making, OSINT has become the core object not only of the government, but also of the many privatized domains and communities of practice. OSINT analysis involves a wide range of tools of trade and best practices that are determined and tailored according to the profile, needs and objectives of each domain.

But what's even more important in the context of security becoming a collective responsibility, is that OSINT allows intelligence stakeholders across the broader IC to engage in the development of joint methodologies. For this purpose, building across communities of practice serves as the foundations for a symbiotic bridge where practice and academia ideally merge and create solutions to solve old and new issues rather than consider them as mere abstract ideas. By bringing together academia, government and private sector one acquires multiple points of views that allow all parties involved to improve and tailor tools for discovering, developing and delivering timely information on threats and risks, overcome biases and mindsets, solve old issues and debates while, at the same time, create solutions to improve and develop the intelligence analysis as a profession.

We expect that the information presented in this volume sparks debates and helps in the formulation of new research agendas. The intelligence studies literature is lacking new material and is in urgent need of revamping itself; there is also a need to tackle the domain-dependence by scholars, not just practitioners. As Benjamin Franklyn once stated "being ignorant is not so much a shame, as being unwilling to learn;" academics need to start looking towards other industries where intelligence is practiced in order to learn more about the profession. Academics write about debates on how it has been impossible to bridge the gap between practice and scholarship; however, if these efforts have been thus far unsuccessful, why not look elsewhere? The private sector intelligence community is young, flexible and it is expanding. Why not approach these organizations? Why limit academia to one domain? Is it mere ignorance that is causing academics to neglect the existence of intelligence practices outside of government? Or, is it the unwillingness to learn? Regardless of this, we want to dedicate the knowledge presented in this issue to all the academics. We hope this serve you all as an awakening call.

Acknowledgments

The authors would like to thank Dr. John Nomikos, the Chief Editor of the *Journal of Mediterranean and Balkan Intelligence* who entrusted the authorship of the December Issue (Volume 10:2) to them. They are also deeply grateful to Dr. Stephen Marrin for the feedback provided during the presentation of this project during the 23rd edition of the international conference *Intelligence in the Knowledge Society Conference* organized by the "Mihai Viteazul" National Intelligence Academy of the Romanian Intelligence Services (SRI) in October 2017. Sincere thanks also go to all the contributors who accepted the invitation to share their expertise and research.

Ms. Daniela Bacheș also acknowledges the support provided by a grant of the Romanian National Authority for Scientific Research and Innovation, CNCS – UEFISCDI, project number PN-II-RU-TE-2014-4-1669, during her 2017 affiliation with the "Mihai Viteazul" National Intelligence Academy.

Endnotes:

01_ See Helene L. Boatner, "Sharing and Using Intelligence in International Organizations: Some Guidelines". *National Security And The Future*. Vol. 1(2000). Pp. 81-92; John A. Gentry, "Toward a Theory of Non-State Actors' Intelligence". Intelligence and National Security. Vol. 31 (2006), pp. 465-489; David T. MacLeod, "Laveraging Academia to Improve NGO Driven Intelligence". Journal of Conflict Studies. Vol. 29 (2009). Available online at https://journals.lib.unb.ca/index.php/jcs/article/view/15236/19649.

02_ Christopher A. Kojm, "Global Change and Megatrends: Implications for Intelligence and Its Oversight". Chapter 4. Zachary K. Goldman, Samuel J. Rascoff (Eds.), *Global Intelligence Oversight. Governing Security in the Twenty-First Century*. Oxford University Press, 2016. p 112

03_ Efren R. Torres, "Welcoming the New Age of Intelligence". *Journal of Mediterranean and Balkan Intelligence*. Vol. 10 (2017).

04_ Robert M. Clark, *Intelligence Collection*. (CQ Press, 2013), p. 40.

05_ For a more comprehensive presentation of intelligence privatization, see: Damien van Puyvelde, "Privatisation". In Dover, R., Dylan, H. and Goodman, M. S. (Eds.), *The Palgrave Handbook of Security, Risk and Intelligence.* Palgrave Macmillan, London, 2017, pp. 297-313. A. Krishnan, "U.S. Intelligence Outsourcing and Its Future". *Brown Journal of World Affairs* Vol. 18:1 (2011), pp. 195-211. Glenn J. Voelz, "Contractors and Intelligence: The Private Sector in the Intelligence Community". *International Journal of Intelligence and CounterIntelligence*, Vol. 22:4 (2009), pp. 586-613.

06_ Myres S. McDougal, "The Intelligence Function and World Public Order". Faculty Scholarship Series. Paper 2569, 1973, p. 382. Available at http://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=3607&context=fss_papers .

07_ Helene L. Boatner, "Sharing and Using Intelligence in International Organizations: Some Guidelines". *National Security And The Future*. Vol. 1(2000), pp. 81-92;

08_ See Smith Hugh, "Intelligence and UN Peacekeeping". *Survival,* Vol. 26:3 3 (1994).

Peacekeeping Intelligence. UN Policy Paper, 2017. Available at http://dag.un.org/bitstream/handle/11176/400647/2017.07%20Peacekeeping%20Intelligence%20Policy%20%28Final%29.pdf?sequence=4&isAllowed=y

09_ Gender Equality in UN Peacekeeping Operations. UN DPKO Policy Directive, 2006. Available at http://www.un.org/en/peacekeeping/documents/gender_directive2006.pdf .

10_ Sean Aday, Steven Livingston, "NGOs as intelligence agencies: The empowerment of transnational advocacy networks and the media by commercial remote sensing in the case of the Iranian nuclear program". *Geoforum*, Vol. 40 (2009), pp. 514-522.

11_ Ellen B. Laipson, "Can the USG and NGOs Do More? Information-Sharing in Conflict Zones". Studies in Intelligence. Vol. 49:4 (2005).

12_ David T. MacLeod, "Laveraging Academia to Improve NGO Driven Intelligence". *Journal of Conflict Studies*. Vol. 29 (2009). Available online at https://journals.lib.unb.ca/index.php/jcs/article/view/15236/19649.

13_ Stephen Marrin, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. Routledge, 2012, 192p.

14_ William O. Odom, Christopher D. Hayes, "Cross-Domain Synergy Advancing Jointness". *JFQ*, Vol. 73: 2 (2014), pp.123-128.

15_ Ibid.

16_ Ibid.

17_ Thomas A. Garin, "Approaising Best Practices in Defense Intelligence Analysis". Russell G. Swenson (ed.), *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Center for the Strategic Intelligence Research, 2003, p.91.

18_ Karen Lund Petersen, Vibeke Schou Tjalve, "Intelligence expertise in the age of information sharing: public–private 'collection' and its challenges to democratic control and accountability". *Intelligence and National Security*. 2017.

19_ Ben Gilad, "Developing Competitive Intelligence Capability," Association of Accountants and Financial Professionals in Business. (2016). Available at: https://www.imanet.org/ /media/58818383cf5b47a4a5229193bcdcb366.ashx.

20_ James A. Barry, Jack Davis, David D. Gries, and Joseph Sullivan, "Bridging the Intelligence-Policy Divide". Studies in Intelligence. Vol. 37:3. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol37no3.

21_ Stephen Marrin, "Understanding and improving intelligence analysis by learning from other disciplines". *Intelligence and National Security*. Vol. 32:5 (2017), pp.539-547.

22_ *Intelligence and National Security*. Vol. 32:5 (2017).

23_ *Intelligence Analysis: Behavioral and Social Scientific Foundations*. National Research Council. 2011. Washington, DC: The National Academies Press.

24_ Thomas Fingar, "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods". Chapter 1. *Intelligence Analysis: Behavioral and Social Scientific Foundations*. National Research Council. 2011. Washington, DC: The National Academies Press.

25_ Patrick F. Walsh, Intelligence and Intelligence Analysis. Willan, 2010, 352p.

26_ Ibid.

27_ Ibid, Chapter 2.

28_ Efren R. Torres, "Welcoming the New Age of Intelligence". Journal of Mediterranean and Balkan Intelligence. Vol. 10 (2017).

29_ National Research Council. 2011. *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences. Washington*, DC: The National Academies Press,

p. 63.

30_ Ibid., p. 1.

31_ Stephen Marrin, *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice*. Routledge, 2012, 192p.

32_ Ibid., p.1.

33_ See Kathleen M. Vogel et al., "The Importance of Organizational Innovation and Adaptation in Building Academic–Industry–Intelligence Collaboration: Observations from the Laboratory for Analytic Sciences". *The International Journal of Intelligence, Security, and Public Affairs*. Vol. 19:3 (2017), pp. 171–196. Karan Jani, "The Promise and Prejudice of Big Data in Intelligence Community". Cornell University Library, 2016. Available at https://arxiv.org/pdf/1610.08629.pdf . Kathleen M. Vogel, Christine Knight, "Analytic Outreach for Intelligence: Insights from a Workshop on Emerging Biotechnology Threats". *Intelligence and National Security*. Vol. 15:4 (2014), pp. 1-18.

34_ Office of the Director of National Intelligence, "Intelligence Community Directive 205: Analytic Outreach", 16 July 2008, pp.1–6. Available at https://fas.org/irp/dni/icd/icd-205.pdf .

35_ Nick Hare, Peter Coghill, "The future of the intelligence analysis task". *Intelligence and National Security*. Vol. 31 (2016), p. 858.

36_ Chriss Pallaris. Open Source Intelligence: a Strategic Enabler of National Security," in CSS Analyses in Security Policy, vol. 3: 32 (2008). To be pasted before the web link.http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/CSS-Analyses-32.pdf