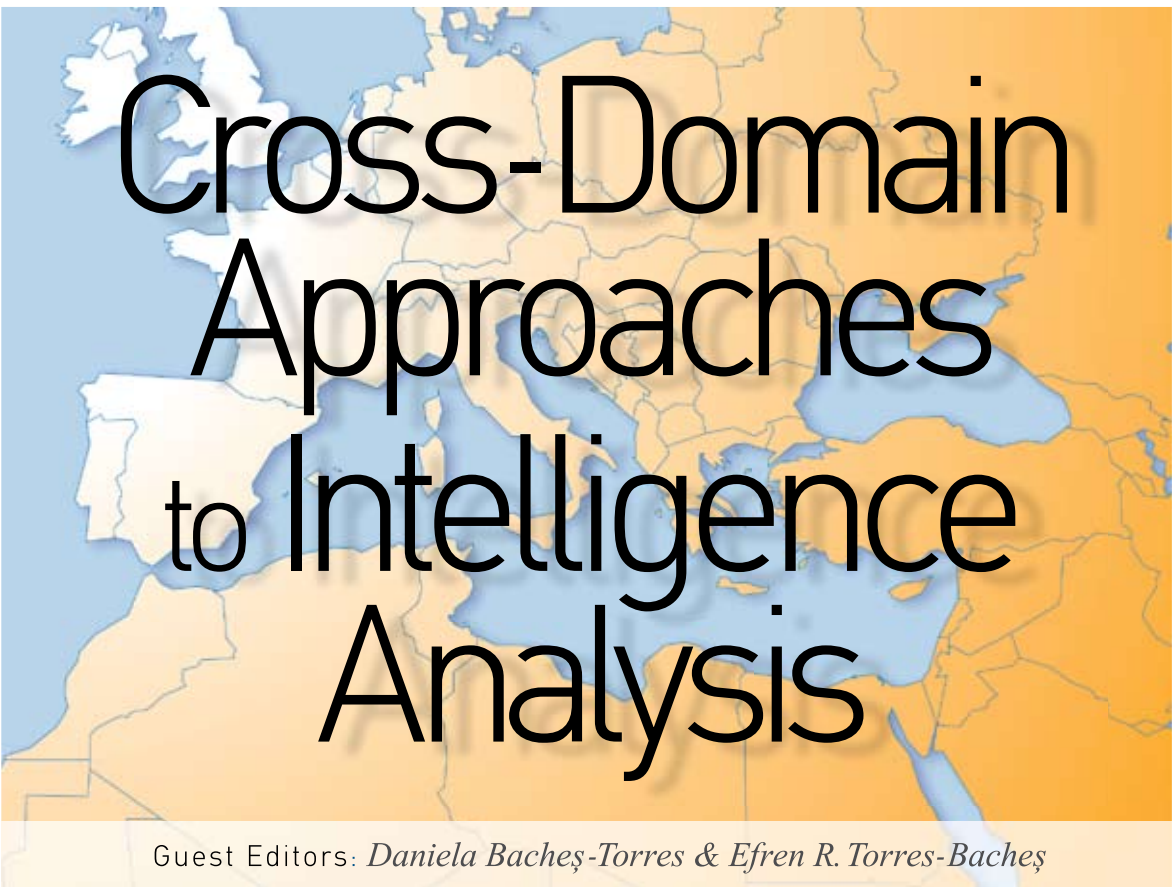
Volume 10 | Number 2 | December 2017 | ISSN 2241-4991

JOURNAL of MEDITERRANEAN and BALKAN INTELLIGENCE



Cross-Domain Approaches to Intelligence Analysis

Guest Editors: *Daniela Bacheș-Torres & Efren R. Torres-Bacheș*

RIEAS
RESEARCH INSTITUTE for EUROPEAN and AMERICAN STUDIES

JOURNAL *of* MEDITERRANEAN *and* BALKAN INTELLIGENCE
AN INTERNATIONAL JOURNAL

Sponsored by the ***RESEARCH INSTITUTE*** *for* ***EUROPEAN*** *and* ***AMERICAN STUDIES***

JOURNAL *of* MEDITERRANEAN *and* BALKAN INTELLIGENCE

AN INTERNATIONAL JOURNAL

Volume **10** | Number **2** | 2017

Guest Editors: *Daniela Bacheș-Torres & Efren R. Torres-Bacheș*

JOURNAL *of* MEDITERRANEAN *and* BALKAN INTELLIGENCE
AN INTERNATIONAL JOURNAL

Sponsored by the *RESEARCH INSTITUTE for EUROPEAN and AMERICAN STUDIES*

Subscriptions:

Individual rate: 100 Euro / 120 US Dollars / 80 UK Pounds
Institutional rate: 200 Euro / 240 US Dollars / 160 UK Pounds

Mission and Scope

The Research Institute for European and American Studies (RIEAS) based in Athens, Greece, publishes the Journal of Mediterranean and Balkan Intelligence (JMBI), which is an international postgraduate academic led-scholarly publication focused on the field of intelligence, counterintelligence, terrorism, counterterrorism, geopolitics and international relations. In the global society we live today, it is important more than ever to work together in order to solve our common problems. The JMBI aims to provide opportunity to young postgraduate scholar to prepare for careers in academic, government, journalism as well as in the private sector. The JMBI is committed to provide an outlet for reasoned intellectual study and the Editorial Team of the Journal hopes to ignite a blaze of future success.

EDITORIAL OFFICE

Dr. John M. Nomikos, #1 Kalavryton street, Alimos, 17456, Athens, Greece.
E-mail at: ***secretary@rieas.gr*** | Tel: ***+302109911214*** | RIEAS: ***www.rieas.gr***

Contents

Editor's Note

The *Journal of Mediterranean and Balkan Intelligence* is a new peer-reviewed journal that addresses a wide range of intelligence issues in the Mediterranean and Balkan region. The journal fills a significant gap in the current study and research of intelligence and is supported by the *Research Institute for European and American Studies* based in Athens, Greece. The *Journal of Mediterranean and Balkan Intelligence* offers a regional perspective of intelligence studies.

The Mediterranean and the Balkans region has assumed a key geopolitical and strategic role since the end of the Cold War, with a long tradition of intelligence spanning over 3000 years. Located at the intersection between Europe, Africa, and Asia, the region has experienced a rapid socio-political transformation over the past two decades. The dismantling of Yugoslavia, the rise of nationalism and political unrest, the Israeli-Palestinian conflict, the proliferation of weapons of mass destruction, international terrorism, religious extremism, migration, maritime security, multinational peace operations, security sector reform, the enlargement of NATO, and the EU, the rise of new regional powers, the discovery of substantial energy resources at sea and the Arab Spring revolutions are only some of the topics that have challenged conventional wisdom and increase the importance of the uses and limitations of intelligence, both for scholars and decision makers at all levels.

These transformations have radically altered the strategic landscape of the region, bringing new security challenges to both local and external actors. Governments are constantly looking for timely and accurate intelligence. Scholars and intelligence analysts need to develop a better understanding of this unstable and conflict-prone region. The *Journal of Mediterranean and Balkan Intelligence* opens a new window to the world of intelligence in this key region.

The journal encourages an interdisciplinary approach to intelligence studies and promotes analyses that use conceptual tools from all major social science discipline – notably, political science, sociology, history, law, ethics, security studies and international relations. The *Journal of Mediterranean and Balkan Intelligence* is published twice a year and invites manuscripts that offer greater intellectual diversity in intelligence-related issues. The Journal aims to serve as a medium for intelligence scholars and practitioners to exchange views on all aspects of intelligence studies and influence both scholarly debates and policy making. The articles included in the journal are based on original research. On occasion, special issues that include guest-edited collections of articles will also be published. We aim to publish articles that make a contribution to scholarship and bridge theory and practice. The *Journal of Mediterranean and Balkan Intelligence* is proud to act as a forum for intelligence scholars and practitioners from around the world.

John M Nomikos
Editor in Chief

We dedicate this issue to our mothers Gabriela and Mariana.

Daniela Bacheș-Torres & Efren R. Torres-Bacheș

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

The Future of Intelligence

Guest Author's Letter

Gregory F. Treverton[i]

A funny thing happened between me preparing to leave the chair of the National Intelligence Council (NIC) at the end of last year and now: Donald Trump was elected president. As I prepared to work and speak about the future challenges of national intelligence, I thought I had a clear view of the issues on the horizon, if not always an equally clear view of what do to about them. Yet here, too, as in almost every aspect of U.S. policy, Trump's election has scrambled the deck, injecting enormous uncertainty. So this list begins with the challenges as I might have portrayed them in more normal times, then concludes with reflections on my puzzlement about how enduring and how momentous the distinctly non-normal times Trump has ushered in will be.

Balancing Strategic and Tactical. This is an enduring challenge; hand-wringing about the primacy of the urgent over the important has characterized all of my years as a student, consumer and sometime practitioner of intelligence. Yet it is made worse by the shapelessness of the current world, which means that every crisis has to be approached afresh on its own terms, and, especially, by the nation's hyper-sensitivity to the terrorism threat. That threat to the United States homeland remains minimal, but that is hardly the way it is perceived by the public – or characterized by politicians. From my perch at the NIC, the acute sensitivity was doubly deforming of our work. When we looked at Nigeria, there was not much Nigeria: it was Boko Haram. And even when we looked at Boko Haram, there was not much Boko Haram: it was all deciphering networks and targeting bad guys. We all wondered and worried, where do these people come from, and why are they doing what they're doing? We did what we could at the NIC trying to understand root causes and motivations. But we were only scratching the surface.

In 2016, the NIC produced about 700 pieces of paper, and more than half of those were memorandums from a National Intelligence Officer to the National Security Adviser, her deputy or another senior National Security Council official. They came directly from the deliberations of the two main policymaking bodies in

i Gregory Treverton stepped down in January as Chair of the U.S. National Intelligence Council, America's interagency group for intelligence analysis, both current support and strategic. Currently, he is Executive Advisor to SM&A Corporation, for which this piece was originally written.

the administration – the Principals Committee, the relevant cabinet secretaries, or, especially, the Deputies Committee, their deputies and the focal point for assessing options and teeing up decisions. Not all those papers were purely tactical. Some were the "what ifs?" of the sort that should be the woof and warp of intelligence-policy relations: "if we do 'x', how will Putin respond?" Because we were at all the policy meetings, we knew what was going on. But my task, every day, was to find time and capacity not just to answer the questions policy officials asked but also to answer the more strategic ones they weren't asking.

Building – and Adjusting – "Stories" in a Shapeless Word. This is a kin of the strategic/tactical challenge, and one that bears more directly on warning. I have come to think that intelligence is ultimately about telling stories, and most "intelligence – or warning – failures derive from holding onto stories that events have outmoded. A story from another realm, Ebola, drives the point home. The medical community had a "story" about Ebola: because death was quick, its period of contagion was brief, thus it would flare up and die out in remote regions. Trouble was that much better transit from rural areas to urban had overtaken the story.

The shapelessness of the world both confounds and demands strategic analysis. If intelligence is story-telling, many of our current stories are suspiciously long in the tooth. In policy terms, for instance, we have been telling ourselves the same story about North Korea for a generation: with just the right combination of carrots and sticks, primarily the latter, and with China as a real partner, we can induce North Korea to foreswear nuclear weapons. Meanwhile, North Korea has gone from an incipient nuclear power to a real one. Intelligence cannot prove and thus cannot say the truth: North Korea is a nuclear power and will remain one; that is all the regime has. But at least challenging the prevailing story would be a start.

For other critical issues, like the Middle East, we have no real story beyond demonizing terrorists and Iran. To be sure, the task is hard. Throughout my tenure at the NIC, I looked for strategic insights and found precious few because the issues are complicated and the causal arrows tangled. The best I found came from our Australian colleagues, who divided the conflicts into three and a half factions – the ISIL-led Sunni extremists: the Saudi-led Sunni autocrats; the Iran-led Shi'ias; and the missing half, the Muslim Brotherhood-led Sunni moderates, recognizing that the term "moderate" is relative at best. But the difficulty of the task is no justification for not trying it. Otherwise, we can all too easily blunder into major campaigns against minor threats or still worse, create those threats.

Transparency and "Big Data." These are two sides of the same coin. The same ubiquity of information that produces so much for intelligence agencies to assess also makes it impossible for their operatives to remain secret for long – and, alas, guarantees that there will be more leaks of methods if not more Snowdens. Perhaps the vision of the future should be more akin to Silicon Valley where

secrets are kept but not for long and where the premium is on collaboration even if today's partner may be tomorrow's competitor.

But that data will be a godsend for intelligence. To be sure, the analytic challenge is greater for intelligence than for private businesses, most of which wants to predict where I will be tomorrow so they can besiege me with ads for things I like. At the NIC, I started an experiment in the Africa account. Its premise was that while there isn't a huge amount of intelligence information on Africa, there is a lot of data out there; the goal was an existence theorem: if the NIC, with a hundred analysts, could make use of data, any place in the Intelligence Community could. Not surprisingly, we found that social media and other available data was pretty good at predicting famine and disease. The next step was to cull "tips" from the data: where should analysts look, what connections should they probe that they hadn't considered.

The NIC also inherited a nifty bid of crowd-sourcing that had been developed by IARPA, intelligence's counterpart to DARPA, the Intelligence Advanced Research Projects Activity. There were two prediction markets, one classified and composed on intelligence professionals and the other unclassified. The open one was the creation of Philip Tetlock, and it had made two important discoveries. Just as some people are better athletes than others, so, too, some people are better predictors; his open market came to feature "super-predictors." Even better, a small amount of training improves prediction. Unsurprisingly, the burden of that training is helping people keep an open mind just a few seconds longer. I used the internal market as a kind of "red cell": if the experts thought development x was y percent likely but the market was betting 2y, what was going on? I didn't care about the numbers, it was the conversation that mattered. And I hoped to move to market from fairly short-run predictions, which could be settled soon, to longer, more strategic questions. For them, I hoped we might create way-stations on which to bet and, in the process, perhaps do better at constructing what intelligence calls "indicators."

Breaking the Cycle. It has been long and often said that the canonical intelligence cycle, from requirements through collection to analysis and dissemination, is often short-circuited. That is true enough – no matter how much intelligence agencies dislike it, policy officials will hanker for the next "raw" spy report or intercept. But as a paradigm the cycle is increasingly unhelpful. In this as in many other ways, what worked tolerably well in the Cold War is dysfunctional now. Then, with one over-arching and secretive foe, it made a certain sense to ask, in a linear way, what we needed to know and how we might collect it. Even analysis had a certain industrial quality about it: a friend who was an NSA Soviet analyst recalls starting the day with a large stack of "her take," the overnight SIGINT collection relevant to her account.

Before I returned to the NIC, I had become a fan of "activity-based intelligence," or ABI. It was developed in the war zones in Afghanistan and Iraq primarily to unravel terrorist networks and identify bad guys. Identifying Osama bin Laden's driver was one of its successes. It amassed information from many sources around particular locations, then used correlations to develop "patterns of life" that would distinguish potential terrorists from ordinary pious Muslim at pray. For me, its side-benefit was creatively disrupting the canonical cycle. It was "sequence neutral": we might find the answer before we framed the question. Think how often in life that occurs; you don't know you were puzzled about something until you find the answer. And in a world of ubiquitous information, ABI doesn't prize secret sources: if information is useful, it's good; if not, not. Finally, perhaps advancing age has made be skeptical of the causation that infuses the canonical cycle. I feel more comfortable with correlation while recognizing that many of the correlations will be spurious.

Intelligence as an Argument for Policy. This, too, is hardly new. In the past, in times of divided government, Congress was tempted to, in effect, turn intelligence issues into policy choices by mandating that if intelligence caught Iran exporting x, then y sanctions would be automatic. To be sure, the practice was more than uncomfortable for intelligence, for it meant asking intelligence to put a gun to the heads of its policy counterparts in an administration! More recently, in days of intense partisanship, administrations have been tempted to use intelligence to argue for their policy choices. So was it in the run-up to the 2003 invasion of Iraq. The intelligence assessment that Iraq had weapons of mass destruction made it difficult for Democrats in Congress to oppose the invasion and provided policy cover for supporting it. So, future administration will be tempted to turn intelligence findings into policy choices: imagine if the Community found what is so far has not – evidence that Iran was persistently cheating on its obligations under the nuclear deal.

New Competitors, New Colleagues. Intelligence has always worried about the competition. A generation ago that was CNN: was intelligence always to be scooped by CNN? (I always thought that concern was misplaced: better to get it right than get it wrong, first.) Now, though, the list of sophisticated private organizations doing "intelligence" is a long one, from Eurasia Group through Bloomberg and Oxford Analytic to Stratfor. The cyber arena is a striking example of the change. In the traditional process, if a major hack occurred, it would fall to the Intelligence Community to attribute it to the perpetrator, then policy would decide on a response, name and shame, seek indictments or whatever. Now, however, that tidy process is disrupted, for while intelligence is doing attribution, so are a host of private companies. And they will not be shy about identifying the perpetrator, never mind what the government might prefer. In the short run, this seems competition; in the long I hope it will become creative collaboration.

Truth as Malleable. So much for my list in normal times. It might be useful, even impressive, for my graduate students. Yet it seems overwhelmed now by the prospect that "truth" will be widely regarded as personal, or political or partisan. Mr. Trump's "false facts" are the poster-child, but the question is how deep and abiding this trend will be. Intelligence, still more than other endeavors, has always known how elusive the truth can be. And our language, like "true enough," is mirrored in the distinction between intelligence and law enforcement: true enough for policy is a looser standard than true enough for a court of law. (In passing, while I've come to admire the marble entrance to the CIA, I've always found the Biblical quotation from John odd and oddly placed there. In fact, and even in intent, intelligence's truth is more likely to constrain policy than to "set it free.") One of the great paradoxes of our times is that all the wonderful technology created to connect people has ended up segmenting them into "echo chambers" in which they hear only what they want and learn only what they already thought.

So far, I see no better response for intelligence than to double down on trying to distinguish what is likely true from what is not. False facts, in principle, make real ones more valuable, and their identification more pressing. The question is: will anyone listen? In the short run and for the Trump Administration, my guess is that the sheer complexity of the issues will continue to turn it toward intelligence and toward a real interest in what is really happening. It is one thing to believe false facts about the turn-out at Inauguration but quite another to believe them while committing GIs to combat in Syria. Or at least I fervently hope so.

The RIS Open Source Intelligence Cycle

Arno H.P. Reuser[i]

Abstract

The intelligence cycle is widely known and used in intelligence studies to explain the intelligence production process, however, the cycle in its classical shape and format is not adequate anymore for the current age. The information landscape has changed drastically, source analysis has become much more important than it already was, the communication circle has changed, the phrase "analysis" is misused and most importantly of all: the concept of customer or client is non-existent in any intelligence cycle. This paper proposes a radically changed intelligence production cycle that at least for Open Source Intelligence processes works much better, where the customer is in the middle, the phrase "analysis" replaced by "synthesis", and where the production speeds is seriously increased by replacing the cycle by a propeller.

Keywords: intelligence cycle, propeller cycle, intelligence production process, information landscape, OSINT, Open Source Intelligence

Introduction

Open-Source Intelligence (OSINT) is mainly involved in the production of intelligence reports based on information found in open sources. However, open-source information has, in the last decades, seen some dramatic changes resulting in serious challenges for OSINT operation. Amongst these are information overflow (also known as information explosion), lack of any validation, fake information, quality control, and information turnover time. As a result, research in open sources has become a tedious process that is more driven by pure luck than by a systematic, planned and structured approach. This article argues that to start developing a uniform, universal

i Reuser's Information Services, Leiden, The Netherlands, http://www.opensourceintelligence.eu. Email: a@reuser.biz.

OSINT process model, a restructured intelligence cycle, specifically for OSINT, is required. The new Reuser's Information Services (RIS) OSINT Intelligence Cycle presented in this paper aims to address a few of the aforementioned challenges and can be the basis for more structured OSINT research methodologies.

Shortcomings and flaws

Most intelligence cycles suffer from the same shortcomings and the same omissions, missing a few important developments in the world of OSINT. These current challenges for OSINT that will be addressed below are:

- Changes in the global information landscape (Sources) ;
- Information overflow ;
- Information turnover time ;
- Information quality ;
- The missing 'customer' ;
- Misuse of the phrase 'analysis'.

a. Sources:

Selecting the right sources for research has increasingly become very difficult indeed due to the following characteristics:

(ι) *Communication circle.* In the previous century, raw data and information was almost exclusively available only via more or less professional information producers[ii]. Information was consumed by users who, typically, did not have direct access to the data. However, due to the information revolution, consumers of information have now also become producers of information. The monopoly of intelligence services on information sources is gone. Because of this, an intelligence service cannot longer simply afford using the obvious open sources for their intelligence products, since their customers have access to the same open sources to solve their information problems. It is worth highlighting that roughly 85% of all required information is found in open sources that our customers have access to just like any intelligence service. Source analysis in an intelligence cycle has become critical. Sources need to be fact-checked, validated, they need to be representative of what is out there.

(ιι) *Information proliferation.* Since consumers of information have also become producers of information, the amount of data has grown

ii Such as radio/TV, press, newspapers, commercial information providers (ProQuest, Lexis-Nexis a.o.), intelligence services, etc.

substantially. Big data, The Internet of Things, the Cloud are a consequence of this. This is what a modern communication pattern looks like: the cellular phone is utilized to record events, Facebook/ Reddit is used to report about said events, Twitter is used to announce it, Flickr/Instagram to quickly publish pictures, YouTube to publish videos, and Periscope to live broadcast video recordings via smartphones. This exponential growth of available information on open sources has been sponsored by the fact that the general public loves to share information about events on various social media platforms.

(ιιι) *Communication patterns.* So many cheap data communication equipment, so many apps and software lead to an unmanageable increase in data formats and communication means that bypass the traditional means of communication such as TV news, books, journals and radio. The finding of people and events demands in-depth knowledge of social media, forums, and discussion groups. Researchers unfamiliar with IRC, Listserv, Usenet and the Deep Web, may miss important information about and by people and events.

As a result, there is an almost endless variety and number of sources available out there. Signals Intelligence (SIGINT) is no longer interesting or relevant since satellite communications are insignificant these days. Image Intelligence (IMINT) is something anybody can do with modern drones. Books are outdated and have been replaced with e-book readers and other mobile electronic devices. Overall, other communication channels have taken over, new kinds and types of sources pop up almost every day, many of those requiring technical skills to make use of them. Many, if not most, of the possible relevant sources are completely unknown to intelligence analysts. Finding and using sources is today's task for specialists.

b. Information overflow:

Sometimes called information explosion or document explosion, the information overflow is a phenomenon that intelligence analysts, researchers and OSINT users are familiar with. The points mentioned above add to this phenomenon to a point where there is no more storage space available for all that data, where researchers get hopelessly lost on the Internet, where the use of scientific libraries is a thing of the past. There is so much information out there, finding the pearls is almost impossible. Researchers get lost, wasting time and money.

c. Information turnover time:

Now that there are so many inexpensive communication channels and communication equipment such as mobile phones, tablets and other mobile devices, the rate in

which information is propagated has increased dramatically, yet most traditional information providers are lagging behind dramatically. Newspapers still work on a 24-hour news cycle, either in the morning or in the evening but not in between. Radio news bulletins are often just once an hour and only cover the most popular items. TV News channels mostly only cover popular events. It is not uncommon to be fully informed about some environmental disaster via modern communication channels instantly. The information turnover time is much faster than it just to be.

d. Quality:

Now that consumers have become producers of information, there is no more quality control of information. A peer-to-peer system does not exist in free Internet information, nor is there an organizing body acting like an editorial board, a series editor, or anything resembling that. The amount of junk data is thus enormous.

e. The lack of the concept ”customer”:

Although all intelligence production is ultimately aimed at serving the customer, almost none of the existing intelligence cycles explicitly mention the customer. Without a customer, no intelligence work makes any sense. It could be argued that the customer is left out because intelligence needs to be completely independent, but that seems like a simple excuse. At the end of the day, it is the customer who decides what the intelligence machinery needs to address.

f. Intelligence analysis:

Intelligence analysis is usually just a single step in the classical intelligence cycle. This is not a very adequate representation since analysis is done in almost every step in the cycle. It is therefore time to change the term analysis to something else and put it in its proper place.

All intelligence production is based on a thorough and in-depth analysis of the information requirements. The assumption in a traditional intelligence cycle is that nothing significant will happen between the first step and the last step. There are no major (inter)national developments that may influence the original requirement; there is no intermediate feedback whatsoever to the customer who has no chance to change the initial information requirement. The world has come to a standstill. An intelligence production process presented in a circle thus does not make a lot of sense. Some essential steps in intelligence production are missing from the intelligence cycle, amongst them: indexing, monitoring, and presenting/briefing.

Current intelligence cycles

The intelligence cycle is traditionally presented as the cornerstone of intelligence production. There are, however, so many variations of 'the' intelligence cycle that it almost looks like that every organization has its own version. Intelligence cycles differ greatly in:

a. The number of steps. Anywhere between four and seven ;

b. Definitions. Definitions of the steps are different. For some, requirement is a separate step, for some it is part of direction.

c. The format. Whereas most intelligence cycles are presented in a circle, some use multiple overlapping circles, or, division halfway the circle.

There is a tendency to criticize the cycle itself as not realistic or as an oversimplified model. Instead of criticizing the intelligence cycle, it may be a good idea to look at the intelligence services that use the cycle. Perhaps the reason for so many cycle variations is that all intelligence services work (very) differently. In the end, one may say there is no such thing as a 'wrong' intelligence cycle; it is a mere reflection of the wide variety of business models that intelligence services use.

For example, the FBI uses a six-step cycle starting with requirements, but does not mention the customers[1]. Their circle and descriptions look much like the one presented by the FAS[2]. The CIA has no need for any requirements whatsoever, they start with planning immediately, apparently not interested in the original requirement[3]. The US Department of Justice (DOJ) is even more interesting, they start the cycle of intelligence production with collecting, not planning and certainly no requirement analysis let alone not even mentioning the customer[4]. The US Air Force cycle ends with feedback and evaluation, but since there is no customer in the cycle, one really wonders where that feedback actually goes to[5].

Intelligence.gov[6] starts with planning too, but requirements analysis is part of: "The process begins with identifying the issues in which policy makers are interested" which is rather remarkable since it should be the customer who identifies the issues, not the provider[7].

Open-Source Intelligence

Before having a look at a proposed RIS Propeller Intelligence Cycle, it makes sense to first define what constitutes OSINT. This is fundamental to understand the newly proposed cycle. Definitions of what constitutes OSINT differ greatly, too. In this paper, the definition of OSINT is as follows:

> *Open-Source Intelligence is a collaborative, integrated methodology and production process where the customers' intelligence requirements are met by providing them with actionable intelligence that is produced*

> *through a process of synthesis and analysis based on a representative[iii] selection of open-source information that is validated, reliable, timely, and accurate.*

The proposed definition of open-source information is:

> *Open-source information or open sources, is all information in any format that can be acquired by anyone without any restrictions, whether for free or commercial, in a legal and ethically acceptable way.*

In the above, however, there are some restrictions:

- Firstly, OSINT is limited by copyright, licensing and other intellectual property rights.
- Secondly, OSINT must also be done completely legal, that is, OSINT does not involve hacking, computer network exploitation, password cracking, etc. of any kind. The open-source information must be obtained legally.
- Thirdly, OSINT should be done ethically. Because truly trained and experienced information professionals can find a lot more than they were supposed to. Open-source information that is not in the public domain or was not intended to be in the public domain does not belong to the area of OSINT. An example of this discussion can be the information published by WikiLeaks. Very interesting information, but since it was not intended to be published, since there is no author or any responsibility that can be hold accountable for the information, it is not exactly known whether the information is original, changed or (in)complete thus that data is not considered as OSINT.
- And lastly, simply collecting and forwarding unedited raw information found somewhere on the Internet is not OSINT.

Another issue that comes into mind is the distinction between OSINT and OSINF. OSINT meaning Open-Source Intelligence, and OSINF meaning Open-Source Information. OSINT is a process of intelligence production; OSINF is an acronym for open-source information. In other words, OSINF is a product/material, OSINT is a process. In the RIS Propeller Intelligence Cycle, the distinction can be clearly seen. Circle one and two lead to a product that may be called an OSINF report. Only when the third circle is used, after thorough analysis of the product, the OSINF report changes into a true OSINT Intelligence report.

With regards to intelligence as a profession, there have been many remarks about OSINT not being real intelligence due to its low rank in the echelons of confidentiality. Classified or unclassified has to do with security and has nothing

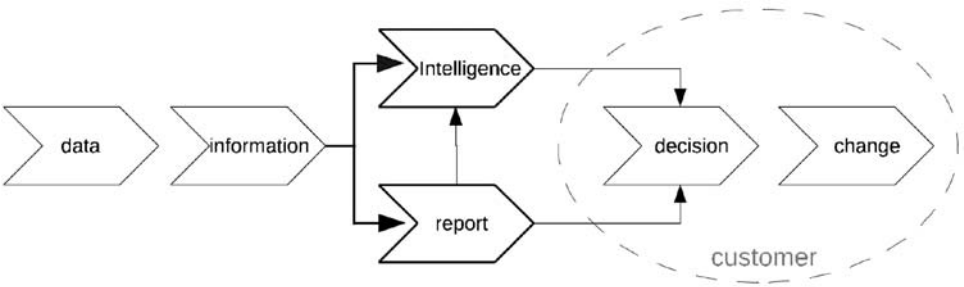
iii Representative in the sense that a source selection should be representative of what's available, representative of different viewpoints, levels, directions, opinions etc.

to do with OSINT. Ideas that OSINT is simply "unclassified information" does not seem to make any sense. OSINF, typically is contained in documents. A document is defined as any object that is intended to derive data from, or is assigned the goal of deriving data from. Examples are books, journals, archeological findings, maps, digital media, but also bricks, broken watches, plastic bags, to name a few. Police investigators can draw a lot of information from criminal evidence regardless the format, thus anything can be a document in that sense.

An intelligence production model

The new intelligence cycle is based on a simple intelligence production model that is important to understand (see Figure 1). The process starts with data. Data is the raw bits and bytes with which intelligence production starts. Data is invalidated, unstructured, duplicated, and chaotic. This data needs to be processed to produce information that is at the very minimum structured, translated, de-duplicated, ordered, decrypted, signed[iv], (maybe) summarized, and validated for usefulness and reliability. Information needs to be analyzed to produce intelligence or some intelligence product. Intelligence should lead to some kind of a decision or at the very least influence a decision which in turn should lead to some change.

Figure 1: RIS OSINT Data - Information model



Two things are important. The first is that, ideally, intelligence must lead to decision and change. Without change, intelligence does not make any sense. The second is that intelligence is the product of what is called 'analysis'. Intelligence is therefore created, never acquired. Any intelligence product sent by agency A to B is a true intelligence product for agency A, but for agency B the product is

iv Which is adding meta data, source descriptions etc. for later retrieval and evidence

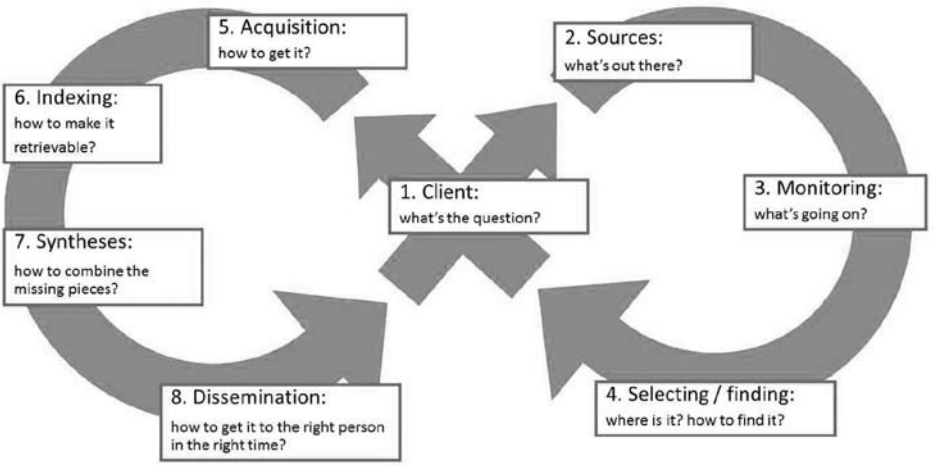
information since B has not (yet) analyzed the product. Moreover, there is also a distinction that need to be considered, between information and intelligence. Since an attempt to define the two will lead to biblical discussions, characteristics are used to make a more or less clear distinction between the two. Information can be characterized in terms of: monitoring, finding, selecting, acquiring, reviewing, cataloguing, reporting, disseminating, informing. Intelligence can be characterized in terms of comparing, understanding, interpreting, explaining, predicting, denying, confirming.

A newer intelligence cycle: the RIS OSINT Roller Coaster

An earlier attempt to create a new intelligence cycle resulted in the RIS ROLLER COASTER (see Figure 2), so called because the intelligence practitioners' work often resembles a Roller Coaster: sometimes fast, worrying and even dangerous, sometimes slow, calm and safe. The Roller Coaster was first presented and explained at the DNI conference back in 2007[8].

Putting the customer as a pivotal point in the middle of operations was already a great improvement to get feedback and maintain a relationship. Also, recognizing that 'analysis' is not just one single step, but that it is done in almost every stage, was important. Hence, the Synthesis phase was introduced instead. But there were still some shortcomings, for instance, the Monitoring phase should be after the customer has given approval to the requirement analysis, not before. An important step, Collection Planning, was not there, and requirement analysis, although in the Roller Coaster, deserves an extra phase. Also, in practice, there is more feedback with the customer than the Roller Coaster suggests.

Figure 2: RIS OSINT Roller Coaster



A newest intelligence cycle: the RIS Propeller Intelligence Cycle

The new RIS Propeller Intelligence Cycle (Figure 3 was developed in 2012 and first presented at the CIISS 2013 conference[9], as well as at OSIRA 2014[10]. Valuable feedback from those conferences, as well as other peers, was used to develop the RIS Propeller Intelligence Cycle.
The Cycle aims to solve a few of the problems and issues raised before in this paper. The Cycle is composed from three interconnected cycles with the customer in the middle:

a. A preparation cycle

This cycle aims to get as much clarity about the research assignment or requirement as possible to make sure the end product meets the needs of the customer. The preparation cycle produces a plan of action which will be evaluated with the customer.

b. A reporting cycle

This cycle consists of five steps were the actual searching and acquiring is done. Information is collated, processed, indexed etc. to produce an information report. The report is evaluated with the customer.

c. An intelligence production cycle

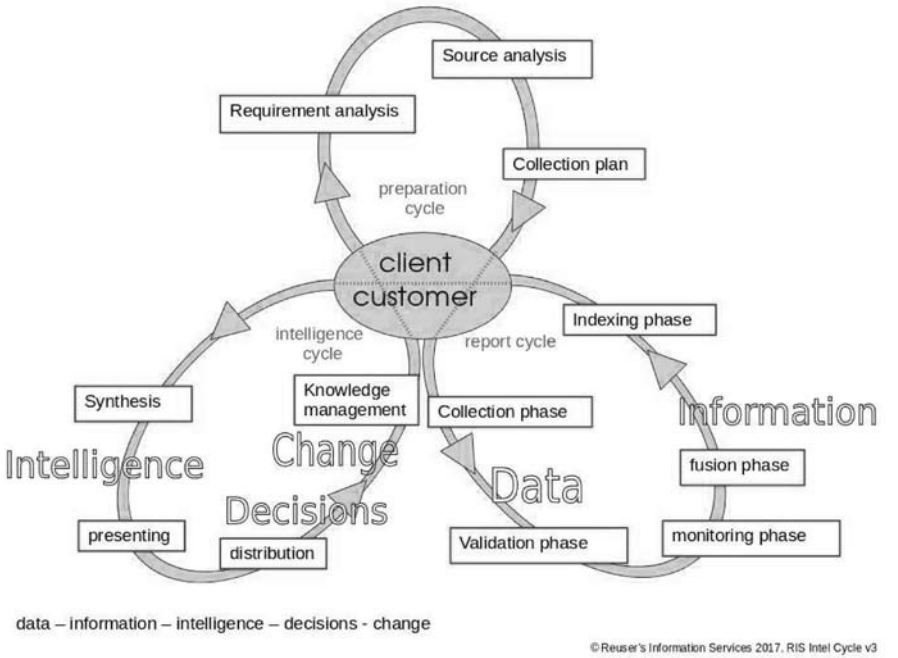
This circle takes the information report and does the actual 'intelligence analysis' bit, produces an intelligence report and distributes it amongst those concerned. Since the customer is the pivot point and the one for who all intelligence is eventually produced, the customer will be in the middle of the new cycle. All sub-cycles start and end with the customer. The customer is now available for regular feedback and reflection.

The Preparation Cycle

The preparation cycle holds three activities: requirement analysis, source analysis and collection planning.
The first phase, requirement analysis, is essential to produce a relevant intelligence report. Breaking down the original requirement into logical steps all help in de-constructing the main problem into sub-problems. Such logical steps include identifying sub-questions, identifying assumptions, identifying and solving variables to prevent misunderstanding with the customer, applying qualifiers to limit and clarify the research process etc., The result of this process is a set of pre-questions that need to be solved (to deal with assumptions and bias), and a set of answerable questions that are defined in such a way that there

can be no misunderstanding as to what exactly needs to be done. Requirement analysis is essential in intelligence production.

Figure 3: RIS Propeller Intelligence Cycle



When there is enough clarity about the tasking, the next phase is source analysis. This phase involves scrutinizing which source to use, establishing reliability and validity of each individual source, making sure the source selection is balanced and representative. As argued before, open sources are too complex to be taken lightly. A separate source analysis step is essential. Knowing what sources to use will also help reducing information overflow. Selection of a relevant, representative and balanced set of sources greatly helps reducing information overflow, since all the researcher needs to do, is to work his way down the list of vetted sources. In addition, getting lost in sources is not a problem anymore.

This will lead to the next step, which is to create a collection plan and a plan of action. This plan lists which sources will be researched in what way (queries, questions) and when. The collection plan will list, following step one and two, the expected answers from each source and the maximum number of results. The plan will also indicate when to STOP searching. This step is an important one in time management and resource management. The plan helps fighting

information overflow because all that needs to be done is to research the sources instead of being overwhelmed by millions of search results from a general-purpose Internet search engine. The plan helps in time management because searching a predefined set of sources can be planned. This step also helps in resource management, because staff can now easily be assigned to specific tasks in the plan.

Another important point is accountability. Working according to the plan and maintaining a progress journal listing activities, searches, queries, results and dates, will help the researcher in being accountable. It will help in continuing the research 'after the weekend' without loss of time or doing things again. It will also help another researcher to continue the research if the original researcher is not available. A collection plan and progress journal is fundamental instruments in intelligence research, thus, step three in the new cycle.

The Feedback I

The product of the preparation cycle is a plan of action that comprises requirement analysis, source analysis and collection planning. It is now time to go back to the customer for verification and approval. The customer can judge if the original requirement is interpreted correctly and if the problem deconstruction is correct. The customer has the option to amend the plan a little (or a lot), propose solutions, propose different sources, give tips and share ideas. This customer feedback is invaluable for the entire process and has the additional advantage of development of a trust relationship. Time has passed since the initial requirement, and maybe new developments have changed said requirements. The customer now has a chance to adjust. This feedback step solves the problem of information turnover time.

If amendments need to be made to any of the first three steps, the Preparation Cycle is run again, until all parties involved are satisfied with the end product. In the latter case, the Report Cycle will start.

The Report Cycle

The report cycle starts with the collection phase of open-source data. The collection phase involves the actual searching for data (or information) and working through the collection plan. This phase also involves the acquisition of the data. This seemingly straightforward phase may have its own issues, especially with government intelligence services where acquisition of information often is a very bureaucratic process, or technical solutions are needed to download and process different information formats, decrypt information, de-duplicate, de-archive, etc.

There cannot be an OSINT unit that works independently. They are all, or at least should, be part of a team. At the end of the day, the analyst is merely interested

in 'good' information; the acquisition channel is less relevant. Therefore, all other acquisition means and sources should be listed here, whether covert or overt. Since this phase is concerned with the information phase of the process, HUMINT is here called HUMINF, SIGINT is called SIGINF and so forth. It is also assumed that each service has a (classified) Book of Sources (an enterprise Domesday Book), each organization should have an extensive list of sources available, how to get access, restrictions, limitations, practical use, etc. The Collection Phase would be ideal to utilize such a book.

Since the Internet contains so much noisy raw information, a validation phase is needed to make reasonably clear that information is reliable, correct, useful, and from the correct source. Each e-mail, each website, each document, should be subjected to the company's validation regime. That regime should be widely agreed, doable, and within reason, simple to apply for all concerned. Validation is vital in today's world and therefor is an extra phase.

The world changes so fast, and because the process of producing an intelligence product can be time-consuming, it may be a good idea to start a monitoring phase at this stage to keep track of developments and make sure that during the process no current relevant developments are missed. If necessary, assuming the interest of the customer is very clear, the researcher may choose to adapt the requirement here or go for extra feedback from the customer. This will also help handling the problem of information turnover time.

Information from all these different sources needs to be processed to remove duplicates, to reformat, to assign Metadata, to discriminate between the relevant and irrelevant srouces, to update the progress journals, add keywords and arrange the information in some meaningful way. The fusion phase is intended for that. This phase produces an information report summarizing the findings in a completely objective way without any interpretation whatsoever.

Obviously, data and information need to be stored in such a way that it can be found back again. Normally, most intelligence services simply dump the information on some network without any indexing at all. At best, some information retrieval program is used, but these are often poorly configured and do certainly not comply with what users need since they are designed and configured by IT personnel, who typically never involve the customer in their projects. The result is a huge collection of private libraries: on paper, digitally and in the personal memories of researchers. A decent indexing process of information is however still such an important phase that it deserves its own step in the cycle.

The Feedback II

The end product of the report cycle is an OSINF report with search results, plan of action, initial findings and an objective summary. The report is not analyzed

in the traditional way. There is no interpretation, explanation, predicting, judgment, just the 'facts'. The report is presented to the customer who can now decide on a couple of things. Either the customer is happy with the information report as it is and does for now not need any further services, or, the customer is less happy with the information report and the report circle will be done again, or, the customer is very happy and requires analysis of the information to produce an intelligence report.

The big advantage here is time. By presenting a report and getting intermediate feedback, the customer does not have to wait until the very end of the cycle to get results. This solves the problem of information turnover time.

The Intelligence cycle

The intelligence cycle consists of three phases: synthesis phase, presenting phase, distribution phase. Since in reality 'analysis' is done at about every step and every phase, using that term as a label for a phase is inappropriate. The term synthesis is proposed as the new term. Synthesis involves all the activities that will produce an intelligence report from an information report: interpreting, understanding, explaining, predicting, summarizing, labeling, judging, etc., in short, all those activities formerly called intelligence analysis. The end product of this phase is an intelligence report[v].

The next step is an often underestimated one: presenting. No matter how good an intelligence product is, if the message is not communicated in the proper way, all effort was useless. So many great intelligence products have been destroyed because the briefer was unable to get the message through, or, destroyed because the author could not express the thoughts properly in a report. A report is too big so that the customer does not read it (properly), poorly written so that the customer misinterprets the text, poorly presented on unclear slides, poorly presented by a speaker, etc. Also, integrity comes into play here. Services either deliberately write vague reports to minimize the risk of 'errors', or on the other side, services write their exact truth which a customer refuses because it is not what the customer wanted to read.

Then, the product needs to be distributed. This distribution phase is another often underestimated step. Whereas the ultimate goal of any intelligence product should be to have the product widely distributed amongst all parties concerned (within reason), quite often services have very strict tables and rules of who get to see which (part of) a report. In addition, intelligence services have a strong tendency to over classify their products so no matter how fantastic an intelligence product is, no one gets a chance to actually read it.

---

v Which can be a textual report, a presentation, a mindmap, a telephone call, a tele-conference, anything.

The final step is knowledge management. At this stage, all the work involved in the production of the intelligence report will be analyzed, labeled, indexed, and stored for future use. The work we mean here is the intelligence analysis methodologies used, the acquisition methodologies used, search strategies, discussions etc. It seems obvious that such work comprise lessons learned (things that worked and things that did not work) and can be used again for a new report, or at least as lessons learned that may be used as input for a next project.

Discussion

We believe that by breaking the OSINT process up in three logical sub-circles, each sub-circle clearly addresses an OSINT research step, and by putting the customer in the middle, the new RIS Propeller Intelligence Cycle functions as a good basis for further research into making an OSINT research process more structured, more planned and more systematic. Further work and research needs to be done in this area to truly develop OSINT into an intelligence production discipline.

The RIS Propeller Intelligence Cycle as it now stands can be applied to many disciplines, but it assumes that the customer is a person or entity that is always actively involved in the intelligence production. That is not always the case, for instance where complete independence of the researchers is required. The RIS Propeller Intelligence Cycle is, despite being formatted as a propeller, still a fairly linear process. It also assumes that all OSINT research can be structured, regardless future developments. The idea that any intelligence research can be modelled may be completely wrong. Perhaps this is the reason why there are so many varieties of cycles out there. Maybe this is also the reason why so many professionals learn about the intelligence cycle, but no one actually follows it in daily practice. Finally, the RIS Propeller Intelligence Cycle does not reflect what the customer has already done themselves, it assumes a strict distinction between customer and support.

Endnotes:

*01_* Intelligence cycle. Tech. rep. https://www.fbi.gov/about-us/intelligence/intelligence-cycle - FBI Intelligence branch

*02_* The Intelligence cycle. Tech. rep. http://fas.org/irp/cia/product/facttell/intcycle.htm. Federation of American Scientists.

*03_* Intelligence cycle. Tech. rep. https://www.cia.gov/kids-page/6-12th-grade/who-we-are-whatthe-intelligence-cycle.html. Central Intelligence Agency, Mar. 2013.

*04_* David L. Carter. "The intelligence process". In: Law enforcement intelligence: a guide for state, local, and tribal law enforcement agencies. Nov. 2004. Chap. 5, p. 63.

*05_* Carl R. Pawling J.O. Miller and Stpehen P. Chambal. Modeling the U.S. Military Intelligence Process. Tech. rep. Presented at the 9th ICCRTS, Copenhagen, 2004. Air Force Institute of Technology, 2004.

*06_* A Dynamic Process Fueling Dynamic Solutions. Tech. rep. http://www.intelligence.gov/mission/how-intelligence-works.html. intelligence.gov.

*07_* Ibid.

*08_* Director of National Intelligence OSINT conference, 16-17 July 2007, Washington D.C., organised by the ADDNI/OS Eliot Jardines.

*09_* The Past, Present and Future of Intelligence / Centre for Intelligence and International Security Studies. - Gregynog Hall, Wales (UK), 23-25 May 2013.

*10_* Inaugural OSIRA conference, 7-8 May 2014, Royal United Services Institute, London, UK.Å

Welcoming the New Age of Intelligence

Efren R. Torres[i] - Bacheș

Abstract

The aim of this paper is to provide an overview of intelligence capabilities in the private sector. Although private intelligence companies such as CACI or Booz Allen Hamilton have a history of offering services to the government, corporations across various industries are opting to establish in-house intelligence units designed to protect their assets. Intelligence continues to be seen primarily as a function of government, but many intelligence professionals are retiring early from the Intelligence Community (IC) and shifting to the private sector. Within the last decade, companies have established intelligence centers as they realize they cannot solely rely on the United States Government and its services to protect their assets. This paper will explore the extent to which intelligence units in the private sector mirror intelligence done in the government. Working primarily with Open-Source Intelligence (OSINT), analysts in the private sector are challenged to find data that may impact their company – physical threats or in the cyber realm. The processes behind collecting and analyzing intelligence is not much different than in government. Various companies adhere to the traditional notion of the intelligence cycle, i.e. the intelligence unit

---

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

I want to dedicate this article to my wife, Daniela Bacheș-Torres, who was very supportive and engaging throughout all the stages of this paper/project, which included: brainstorming, academic exchange of ideas and the proper structuring of the argument presented here as it was briefed to the audience at the Intelligence in the Knowledge Society Conference organized by the "Mihai Viteazul" National Intelligence Academy of the Romanian Intelligence Services (SRI) in October 2017. This paper could not have been possible without her encouragement, unconditional support, and expert advice."

has requirements and guidance, a collection plan, analysis and exploitation of sources and subsequent dissemination of information to decision-makers. It is likely that in the coming years, additional companies will develop intelligence units to mitigate the impact of emerging threats worldwide.

Keywords: Private Sector Intelligence; Intelligence Cycle; Competitive Intelligence; Open-Source Intelligence; Evolution of Intelligence

Introduction

Intelligence as a profession has always been strictly thought of as a function of government to protect the homeland. While intelligence was born out of the need to protect society and avoid surprise from enemies since well before the era of Sun Tzu, within the last few decades, private companies have taken initiative to adopt said intelligence functions to protect their members of staff and assets worldwide. In addition to this new initiative by the private sector, a new trend is emerging where members of the United States Intelligence Community (USIC) are retiring from their governmental roles and joining the private sector as managers for the various new intelligence units being established. As a result, the private sector is benefiting from the extensive network of USIC contacts that these former government employees bring along with their experience, which is contributing to the crafting a new Private Intelligence Community (PIC) that relies mainly on the OSINT tradecraft.[ii]

Per Allen Dulles's early claim on the ratio of intelligence collection, approximately 80% of all intelligence is found in open sources[i] (foreign media, social media, etc.). This has allowed the private sector to assemble their own intelligence units, which rely on OSINT, Social Media Intelligence (SOCMINT) and, to some extent, on Human Intelligence (HUMINT). The implementation of these types of intelligence collection practices are giving the private sector the edge it needs to compete with the USIC. Due to this new development of intelligence functions in the private sector, companies are starting to expand operations to medium and high-risk countries, which makes it far more challenging for them to monitor and report real-time intelligence to company stakeholders. Because of this challenge, PSIUs are opting to engage with third-party vendors that have specialized services such as on-the-ground intelligence (Human Sources) and

ii The following discussion will be based on available and relevant literature as well as expertise, interviews and know-how from the author's extensive experience practicing intelligence in the private sector. The aim of this work is to create an explicative narrative of the existing intelligence units in the private sector. This work does not aim at debating or touching on theories that currently exist in the intelligence studies literature. In addition, the information collected and presented in this work derives from information publicly available from private intelligence companies as well from personal experience. It is necessary to state that all the information presented here does not represent the views or opinions of any private company in the United States of America.

real-time GPS tracking. The inclusion of third-party intelligence companies provides PSIUs with other valuable and privileged resources outside of the OSINT realm.

Unfortunately, yet not surprisingly, despite the expanding role of traditional intelligence in the private sector, academia has not vested resources or the time to study the similarities, differences and dynamics in said profession. The perception of many private sector intelligence professionals is that academics tend to associate traditional/protective intelligence in the private sector with competitive intelligence done in the business world. Competitive intelligence identifies risks and opportunities to allow a company to adapt its marketing or sales strategy or in extreme cases, change it.[2] It is essential that intelligence scholars invest the time to study the different PSIUs from top companies to further develop the intelligence literature. For this reason, this paper is designed to make a contribution by facilitating interest and delivering information about the growing existence of PSIUs.

This paper will define private sector intelligence and will expand and explain the role of traditional intelligence applied to the corporate world, while, at the same time, showing a clear outline that maps the future of intelligence outside of government.

Between Public and Private: (Re) Defining Intelligence

Intelligence has an inherent definition problem, and many former practitioners and academics have attempted to define it. While the Intelligence Community (IC) favors more 'in-the-field' definitions, academia has tried to come up with a more ambitious approach aimed at embedding the multiple facets of intelligence. According to the Commission on Organization of the Executive Branch of the Government, intelligence is anything that "deals with all the things which should be known in advance of initiating a course of action."[3] The 2001 Joint Chiefs of Staff's Department of Defense Dictionary of Military and Associated Terms, on the other hand, focuses on intelligence rather as a product, as "information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.[4] On the academic side, most of the scholars engaged in such an endeavor have tried to catch the broader landscape. Mark Lowenthal defines intelligence as "the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and his information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.[5] Others have also looked at the intelligence organizations as agents providing the frame of reference for understanding intelligence. Abram Shulsky explains that intelligence activities are conducted by organizations that have something

in common: they have as one of their "most notable characteristics…the secrecy with which their activities must be conducted."[6] All these definitions revolve around intelligence being a function of government and as a process only strictly applicable to national security matters. Because Intelligence Studies is still developing, these definitions of intelligence have had a very limited focus, which has led to practitioners and academics to lack awareness of the existence and application of traditional intelligence outside of government and the military.

Intelligence has not always been a practice exclusive to government agencies or the military. Throughout history, successful merchants and businessmen have engaged in intelligence and security activities.[7] Intelligence as a function outside of government and the military dates back to as early as the 1500s when English spies were sent out to find the secrets behind the Dutch ceramics industry. Furthermore, the entire spice trade of the East Indies was also shrouded in secrecy as thick as any military weapons program for centuries.[8] However, the implementation of intelligence functions to the corporate sector was not contemplated until Stevan Dedijer officially identified intelligence as being a powerful business tool in the 1950s.[9] Nevertheless, although financial institutions had been implementing intelligence collection and analysis of markets since World War II,[10] the application of intelligence to the rest of the corporate world did not start spreading until the 1970s and 1980s as governments were divesting from the private sectors, including mining and transportations, which resulted in the need for companies to rely on their own means to protect their interests.[11] Even then, this migration of intelligence functions to the private sector was simply used as a tool to manage business risks.

Starting in the late 1980s, companies, particularly fuel companies, started to take actions against physical risks and shifted from a business-aimed intelligence function to an approach that resembled more of the traditional use of intelligence.[iii] Furthermore, in years following 9/11, companies began to create in-house intelligence units that were dedicated to the collection and analysis of intelligence on physical, reputational and cybernetic threats that could affect an organization or industry. This pioneering initiative was furthered amplified by the transition of USIC professionals from government to private companies. These former USIC practitioners are in part responsible for shaping and defining what these PSIUs are becoming. Despite the spreading of PSIUs among many private companies, there is still a general misconstrued differentiation between traditional intelligence in the private sector from Competitive and Business Intelligence.

Before elaborating on the role of traditional intelligence in the private sector, it is important to differentiate between the two dominant types of intelligence

iii This was gathered from interviews with private intelligence professionals.

existing in the corporate world: Business Intelligence and Competitive Intelligence. According to Katarina Lagerstam, Business Intelligence (BI) constitutes the intelligence needed to run a business organization.[12] BI uses a derived model of the intelligence cycle to ensure the survival of the company.[13] Although BI has adapted a similar intelligence cycle from that of government, it focuses on gathering information on markets, product strategies, competitors and socioeconomic forces that may impact the success of the business. BI utilizes competitor analysis/profiling and/or analysis of the environment to ensure a successful business venture.[14] Jan P. Herring describes BI departments as having four primary objectives: providing early warning to prevent surprises and identify threats; to support the strategic and operation decision-making processes in companies; to assess the competition and monitoring their activities and lastly, to support the company's planning and strategy formulation processes.[15] The overall objective of BI professionals is to be able to provide actionable intelligence for effective business decisions.

Competitive Intelligence (CI) is defined as the collection of data solely about competitors, converting this data to information, and applying it to short and long term strategic goals.[16] During the mid-1990s, when CI was still a relatively new discipline, it was estimated that less than 7% of Western companies had operating CI units[iv]; however, this has expanded considerably. Unlike BI, CI solely focuses on gathering open-source information on competitors and, in many on-going cases, remains separated from other organizational research and analysis initiatives like market research or planning and performance management (PPM).[17] CI can also be regarded as a process and not a function; therefore, it should appear in all aspects of the company as a continued action rather than being subjected to one specific department[v].

BI and CI as disciplines or processes are often mistakenly used as interchangeable terms to describe the role of intelligence in the private sector. Conversations of traditional intelligence in the corporate world are lacking. The reason for the lack of awareness of the existence of traditional intelligence in the private sector is the fact that topics on BI and CI dominate the literature, which dates back to the 1990s, and has not been updated to reflect the need for businesses to use intelligence as a strategic tool to protect their assets from physical and cyber threats.

Companies around the world have always monitored factors that affect their business, although perhaps in a more informal, less structured, and in many cases, less conscious manner.[18] Nevertheless, as mentioned before, the evolution of threats following 9/11 forced corporations to rely less on governmental agencies. Because of this, corporations have taken the necessary steps to become more independent by building in-house intelligence units to collect

iv Larry Kahaner, Competitive Intelligence: how to gather, analyze, and use information to move your business to the top. (London: Simon & Schuster, 1998), p. 16.

v Ibid, p. 23

and analyze information pertaining to events and actors that may impact the business. Although the role of intelligence as a protective tool dates back to the 1980s to the oil and gas sector, academics and intelligence professionals have not developed an adequate definition to explain this function outside of the government sector.

Private Sector Intelligence (PSI)[vi] as a practice can be defined as the process of collecting, analyzing and disseminating actionable strategic and tactical information,[vii] obtained through OSINT, SOCMINT and HUMINT sources,[viii] on possible hostile actors and hazardous worldwide events, which may represent a direct physical or reputational risk to a company's operations and assets. The mission of PSIUs is to provide early warning to executives, and other stakeholders, on any perceived threat that may impact a business or threaten its operational existence. Furthermore, additional PSIU responsibilities include providing internal and external threat investigations, risk assessments, high-risk travel monitoring via geospatial trackers, and to liaise with the IC and other corporate entities for information sharing purposes.

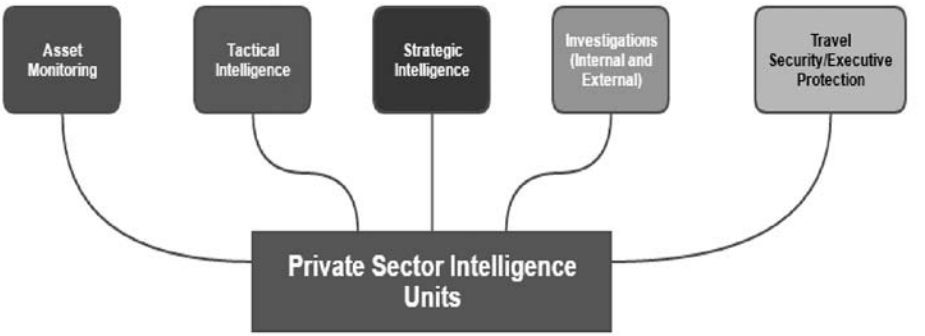


Figure 1: Ramifications of Private Intelligence Sector Units[ix]

vi The term PSI will be used strictly to talk about traditional intelligence applied to the corporate sector and does not include or refer to Competitive Intelligence or Business Intelligence.

vii Actionable information here refers to valuable and concrete information that will help company decision makers to take a course of action regarding the safekeeping of personnel and assets worldwide.

viii This definition is based on demands of intelligence from the Private Sector. Now, even at the government level it is impossible to agree on what intelligence is; nevertheless, this definition is strictly based on the experience by both authors on the needs of PSIUs. Moreover, it is important to state that each PSIU, depending on the company's industry, will have varying degrees of needs. For example, an insurance company such as AIG will have different collection needs than an entertainment company such as Disney or Paramount Pictures.

ix This graph was developed by the author.

Core Competencies of PSIUs[x]

Open intelligence sharing is a luxury enjoyed by the corporate sector, and although companies do possess proprietary and sensitive information that needs to be protected, depending on the industry, they are also willing to share vital intelligence on threatening actors, through benchmarking, with other like-minded organizations. The advantage that PSIUs have is that information can be shared instantaneously without the inconvenience of bureaucratic counterintelligence protocols. In the United States, the government has facilitated information sharing through various platforms designed to bring together the private sector to cooperate with the public sector. A strong example of this is the New York Police Department (NYPD) Shield program, which is an umbrella initiative for a series of current and future police department efforts that pertain to private sector security and counterterrorism; Shield is described as a public and private partnership based on information sharing.[19] Additionally, another interesting NYPD project is the Lower Manhattan Security Initiative (LMSI) designed to increase surveillance efforts in Lower Manhattan in New York City.[20] LMSI brings together the NYPD and private surveillance capabilities to ensure the safekeeping of the population.[21] Furthermore, a well-known existing government body that facilitates information sharing is the Overseas Security Advisory Council (OSAC), which promotes security cooperation between American private sector interests worldwide and the U.S. Department of State.[22] Both NYPD Shield and OSAC brought together American companies participating or sponsoring the 2016 Summer Olympic Games in Rio de Janeiro, Brazil. These government bodies served as a channel for various companies to share intelligence relating to cargo theft, cartel/gang activity and the possible threat of terrorism during the event. These platforms helped PSIU Subject Matter Experts (SMEs) address industry-specific threats.

Members of the leadership team in PSIUs most likely possess experience from within the USIC. As a matter of fact, corporations have intentionally placed former government and military personnel in managerial positions as they bring a wealth of experience, knowledge and a vast network in both the private and public sectors. These former government and military employees do not only bring knowledge and contacts, but they have been responsible for implementing a solid structure to many corporate security departments. Consequently, the leadership structure in PSIUs mirrors, to some degree, that found in government and the military, which provides a clear chain of command. A top-down organizational structure gives intelligence analysts a direct point-of-contact for time-sensitive matters and critical incidents, which simplifies communication channels and eliminates confusion during fast-paced responses to a major incident such as a terrorist attack.

---

x This sections is based on professional experience in PSIUs by the author.

PSIUs have a unique knowledge repository that encompasses SMEs from various backgrounds, including former government and defense employees, academics and personnel with solely corporate experience. The diversity found in PSIUs allows corporations to address relevant threats. For example, in the healthcare industry, a company may address threats in the form of cargo theft, counterfeited pharmaceutical products for sale on the black market, foreign government regulations, and industrial espionage. Financial institutions may face different threats in the form of insider trading, money laundering, fraud, cyber-attacks and reputational risks when dealing with foreign governments. Every PSIU is tailored to the company's industry and needs, therefore, it needs specific guidelines to respond to perceived threats.

In order to provide a near-complete glance of how PSIUs work, it is necessary to explore how PSIUs engage in their work. Just like any intelligence unit, PSIUs need to establish and adhere to protocols. Protocols may range from incident response during a natural disaster to accounting for executive travelers and company assets during a major terrorist attack. Depending on the nature of the incident, some PSIUs have an expected response time to advise upper management and stakeholders with reports containing the latest intelligence available. Due to the growing international footprint of some corporations, it is imperative to establish protocols that speak to thresholds necessary to trigger a reaction from intelligence analysts in order to gather timely and accurate intelligence on incidents that could adversely affect company assets and personnel.

Cloak and Dagger: PSIUs Capabilities[xi]

The Intelligence Cycle is the basis for ensuring that intelligence practitioners collect and assess information efficiently and effectively in order to provide the most current and precise information. It is important to mention that one strong similarity between PSIUs and government intelligence is the intelligence cycle. PSIUs follow a five-step intelligence cycle similar to that of government that includes Planning and Direction, Collection, Processing, Analysis and Production, and Dissemination.[23] Moreover, as with any intelligence unit and intelligence cycle phase, PSIUs utilize a wide variety of tools and resources that ensure a more comprehensive intelligence collection; these resources can range from unclassified/official government documentation to even HUMINT sources offered through third-party private intelligence companies.[xii] Depending on the

xi This section will be detailed based on professional experience by the author as well as interviews with intelligence professionals working in the private sector.

xii Private intelligence companies refer to companies that exclusively offer security and intelligence services such as IHS, Control Risks, iJet and NC4 Solutions, all whose information is publicly available on their respective websites.

industry, the emphasis and preference on certain types of private intelligence companies and their tools are likely to vary. For example, a healthcare company may lean more towards a company that offers intelligence on threats solely targeting that industry than on other more general political analysis on a region with no company footprint. There is one common denominator across all PSIUs, they use these tools, along in-house subject matter expertise, to provide early warning and strategic advice to the business to act in the event of serious security incident (terrorist attack, insurgency or civil unrest). These third-party private intelligence companies, their information and tools, give PSIUs a complete approach to the application of the intelligence cycle to the private sector, which not solely includes OSINT.

Issues and Debates

As with any practice, there are many issues and debates that can detract from the quality of intelligence that is produced by both the public and private sectors. The first point of contention is the concept of why intelligence fails in the private sector. Is this intelligence failure in the private sector due to actual collection/analysis failure or internal policy failure? It would be naïve to pinpoint a single reason for intelligence failure since it is usually a combination of many factors. However, it is important to note that the emerging organizational culture of the PSI community reflects the tentative hypothesis that the majority of failures are due to internal policies being too rigid to allow practitioners the ability to capture and utilize the intelligence that could be critical for a possible future attack. However, while no literature exists regarding internal policy failure in the private sector, it would be interesting to look at comparisons from similar failures in the government sector and engage into future research on such consistency. One example of how policy failed in the government sector is the time period right after the 1998 bombings of US embassies in Kenya. These bombings provided policymakers an opportunity to recognize and address the growing threat of terrorism against US interests but policymakers failed to implement strategic policy initiatives.[24] Ineffective policy can detract from quality intelligence products if the SOPs prevent the needed flexibility in the intelligence cycle. Not every attack or threat will meet every threshold or criteria, nor will every threat look exactly the same. It is important for supervisors to recognize the need for their analysts to consider some threats that may fall outside the thresholds, as there may be additional intelligence that justifies a critical threat.

Furthermore, the age-old debate of specialist vs. generalist is not an argument that is exclusive to intelligence practitioners. Intelligence analysts in the government sector are specialists as they are given topics to become SMEs for. In government, intelligence managers have yet to recognize that more effective policy support requires the building and maintaining of expertise.[25] USIC retirees

transitioning into the private sector have managed to address the aforementioned issue, needless to say that they have the freedom to do so. In the private sector, analysts are generalists as they are responsible for a wide range of subjects and threats. The fallback with generalists is that the knowledge base is average due to needing to have some understanding of several areas. However, specialists that train in more than one specialty can provide more value in the private sector due to having advanced knowledge and training on several subjects.

Moreover, due to federal budget cuts as well as lengthy hiring processes, government agencies have taken to outsourcing intelligence to contractors for a fraction of the cost. The debate regarding outsourcing intelligence to contractors or only hiring internal staff is whether the agency is still receiving quality intelligence. A hired contractor is likely making less than their equivalent internal staff counterpart and is often working on a limited basis due to the terms of the contract. This leads to contractors lacking a sense of loyalty for the agency, as contractors do not have access to the same benefits, salary, and career opportunities. Quality intelligence can suffer from discontent of contractors or friction among contractors and staff. Intelligence can also suffer due to high turnover rates and the constant hiring, onboarding, and training of new contractors. An unnamed government agency utilized a company that hired one hundred intelligence contractors. Less than 10% of contractors stayed longer than one year.[26]

When it comes to the dialogue between consumers and producers of intelligence, applied intelligence to the private sector is a thriving example of Sherman Kent's argument regarding analysts being too close and too far away from policy-makers. As Kent stated in his final chapter of *Strategic Intelligence,* policy-makers and analyst relationships are of utmost delicacy.[27] The relationship between intelligence analysts and policy-makers is important; however, in private companies, this relationship is more flexible and open. In the private sector, analysts are part of the process that prescribes policy thus PSIUs have more freedom to tell truth to power. Although academics may take this as a source of bias, it is necessary to establish that intelligence, as a profession, is inherently a biased profession.

That being said, PSIs and their relationship to stakeholders are founded on a thin layer of ice, but in a more sensitive manner than in government. Intelligence units in the private sector do not generate any revenue and are subject to cuts in personnel and capabilities. This is an important parallel with the IC as different agencies compete for federal funding. Intelligence, however, will always be a tool of wondering: if attacks are prevented, how do we know they were, indeed, prevented? If attacks do happen, why did we not prevent it? As once mentioned by John F. Kennedy: "…victory has 100 fathers and defeat is an orphan…"[28]. It is impossible for both government and private sector to measure successes and failures. In the private sector, there is less room for failure than in government.

Failures indicate the eradication of intelligence units while the IC enjoys the security of their respective agency (ies) existence(s). Furthermore, the issue of cloak and dagger will never leave the profession as it is inherent and native to its existence. PSI and Intelligence are first cousins, which enjoy and suffer from the very same familiar issues: budget competition, contractors' lack of loyalty, etc. Will these issues ever be solved? Most probably they will not; however, academia can assist in opening a discussion about these issues.

Academia and Private Sector Intelligence

Unfortunately, intelligence academics have paid little to no attention to the private sector, predominantly due to the misconception that intelligence is just pertinent and relevant to a government function, and that intelligence can only be applied to the private sector in the form of Competitive and Business intelligence. PSI thrives from the very same tradecraft that drove Moses's spies and Sun Tzu to collect and analyze information on their adversaries. Academics have scrutinized government failures and have condemned the USIC and the international IC for having a failure of imagination, and for not being able to prevent early warning to attacks. Notwithstanding, academics have become victims of their own critiques. Although intelligence was born out of the necessity to be one step ahead of the enemy, it has evolved to adapt to the needs of the corporate world as well. Academics are likely to continue criticizing the IC for not being able to predict attacks. Until intelligence scholars realize that they are leaving out a very important and evolving aspect of intelligence (PSI), the issues and debates will continue to be the same, just in different words, prose, and with new academic references.

An effort to step out of the academic comfort zone is the Early-Career Scholars Group (ECSG), which is a pioneering initiative and example of online platform/network dedicated to advancing intelligence studies that incorporates government, military and private sectors.[xiii] Nevertheless, it lacks the attention and interest in intelligence away from the government domain from all scholars involved. A constructive critique to ECSG academics is that they do not realize that the government is limited to OSINT and HUMINT - as well as every other intelligence collection domain mentioned in the literature - and that it [intelligence in government] is tied by counterintelligence protocols, which understandably limits the engagement of intelligence practitioners with foreign parties; however, private sector intelligence analysts have the ability and freedom of moving everywhere. PSIUs have covert, overt and privileged sources. In PSI, analysts,

xiii The Early Career Scholars Group (ECSG) in Intelligence Studies is an emerging network of a new and younger generation of researchers created at the end of 2016 under the auspices of the Intelligence Studies Section at the Intelligence Studies Association. The ECSG is aimed at engaging the new generation in collaborative research projects between government, military and private intelligence practitioners and academia.

have the freedom of establishing and nurturing relationships with foreigners without counterintelligence concerns. Intelligence analysts liaise with assets (academic or experts), establish relationships and exploit information through social engineering. Academia must realize that PSI has a bigger and richer network of contacts that encompasses the government, military, academics and industry partners; scholars must also realize that private sector successes and failures are openly available without any level of classification (for the most part). If academics could scrutinize and examine PSIUs and their respective successes and failures, there is no doubt that there will be a more robust information repository from which all parties can benchmark from, which then can lead to the establishing of a new and more direct research agenda for academics. This means advancing and evolving towards a more comprehensive understanding of the intelligence practice in all platforms in which it operates.

Concluding Remarks

The intelligence practice is constantly evolving to keep up with emerging threats, developing technology, and forms of intelligence gathering. The growth of the intelligence field also comes with the transition of Government Intelligence to Private Sector Intelligence. PSIUs are becoming more prevalent with the implementation of intelligence gathering in the private sector, yet the literature remains extremely limited and solely focused on government failures. By defining PSI, practitioners in the field of Intelligence can have clear guidance of how to apply traditional intelligence to corporate settings. The future of PSI will rely heavily on OSINT and SOCMINT tools to provide quality intelligence, which will help shape the future of intelligence sources.

Many PSIUs are new and are starting to learn how to create their own operations, thresholds, protocols, and own networks with the Intelligence Community and Law Enforcement to increase intelligence sharing capabilities. PSIUs are developing their own corporate intelligence networks, capabilities, training and standards. Furthermore, PSIUs are changing the nature of the intelligence practice through innovative ways of collecting, analyzing and sharing information that steer away from traditional intelligence practices. The new breed of analysts that thrive in an environment where OSINT and SOCMINT have become valuable sources have become the gatekeepers of information in the new era of intelligence, and academia could highly benefit from studying them. The developing of Intelligence Studies is a back and forth conversation between the government and academia that urgently needs to start incorporating the corporate sector, otherwise it will be limited to overly analyze past failures and will miss valuable opportunities to branch out to a new turf and develop its literature. With the growth of PSI, there are also unique challenges that need to be addressed, such as the need to deeply scrutinize internal policy

failures, difficult transitions for former federal employees to corporate culture, the loyalty of contractors, and whether PSIUs require generalists or specialists. These issues will need to be addressed head on in the future, and academia, as an important partner in this discussion, is encouraged to inquire and explore more into this area as this profession has already branched out of government functions and has welcomed a new age of intelligence, a brand-new era of spies.

Endnotes:

*01_* Christopher Hobbs, Matthew Moran and Daniel Salisbury, *the Palgrave Macmillan Open Source Intelligence in the Twenty-First Century,* (Hampshire: Palgrave Macmillan, 2014), p. 9

*02_* Benjamin Gilad. ""Competitive Intelligence" Shouldn't Just Be About Your Competitors." Harvard Business Review. May 18, 2015. Accessed August 19, 2017. https://hbr.org/2015/05/competitive-intelligence-shouldnt-just-be-about-your-competitors.

*03_* Commission on Organization of the Exec Olive Branch of the Government (the Hoover commission) Intelligence Activities, June 1955, p 26 This was an interim report to congress prepared by a team on under the Leadership of Gen Mark Clark.

*04_* Joint chiefs of staff, Department of Defense Directory of Military and Associated Terms. Joint Publication, 1-02. 12 April 201, p. 208.

*05_* Mark M. Lowenthal, Intelligence: From Secrets to Policy (Washington, DC: Congressional Quarterly Press, 2002 [second edition]), p. 8.

*06_* Abram N. Shulsky (revised by Gary J. Schmitt), Silent Warfare: Understanding the World of Intelligence (Washington, DC: Brassey's (US), 2002 [third edition]), pp. 1-3, 171-176.

*07_* Stevan Dedijer, Europ's "To BI or not to BE?" Talk at the Societ for the Competitive Intelligence Professionals in Cologne, Germany 1993. Avaliable at: Available at: www.onlinelibrary.wiley.com/doi/10.1002/cir.3880040213/full. Accessed: 24/06/2017.

*08_* Patrick Marren, The Father of Business Intelligence, *Journal of Business Strategy,* Vol:25:6, p. 5

*09_* Pierre Piganoil , "The Emergence of Corporate Intelligence," found in Jon Sigurdson and Yael Tagerud, *The Intelligent Corporation: The Privatisation of Intelligence,"* (London: Taylor Graham, 1992), p.23

*10_* Jan P. Herring, "Business Intelligence in Japan and Sweden: Lessons for the US," *The Journal of Business Strategy,* 1992, p. 315

*11_* Jan P. Herring, "Educating the Next Generation of Intelligence Professionals," Association of Former Intelligence Officers (AFIO) Guide to the Study of Intelligence, p. 557, available at: http://www.afio.com/publications/Guide/index.html?page=605. Accessed on 13/8/2017.

*12_* Katarina Lagerstam , "Financial Intelligence in Foreign Exchange Markets," found in Jon Sigurdson and Yael Tagerud, *The Intelligent Corporation: The Privatisation of Intelligence,"* (London: Taylor Graham, 1992), p.134

*13_* Ibid

*14_* Ibid

*15_* Jan P. Herring , "Th Unique Role of the Future in Intelligence," found in Jon Sigurdson

and Yael Tagerud, *The Intelligent Corporation: The Privatisation of Intelligence,"* (London: Taylor Graham, 1992), p.164

16_ Jack Cooper, Josephine Hamer & Jeanne Schultz, "Competitive Intelligence," *Journal of Hospital Librarianship,* Vol1:3, p. 71

17_ Nanette J. Bulger, The Evolving Role of Intelligence: Migrating from Traditional Competitive Intelligence to Integrated Intelligence," *The International Journal of Intelligence, Security,, and nternational Affairs,* Vol18:1, p. 60

18_ Gustavo Diaz Matey,"The Use of Intelligence in the Private Sector," *International Journal of Intelligence and Counterintelligence,* Vol:26:2 (2013), p. 277

19_ "About." NYPD SHIELD. http://www.nypdshield.org/public/about.aspx. Accessed July 10, 2017

20_ Hogarty, Dave. "Downtown Surveillance Network Proceeds." Gothamist. September 7, 2007. Accessed November 12, 2017. http://gothamist.com/2007/09/07/downtown_survei.php.

21_ Buckley, Cara. "New York Plans Surveillance Veil for Downtown." The New York Times. July 08, 2007. Accessed November 12, 2017. http://www.nytimes.com/2007/07/09/nyregion/09ring.html?_r=1&adxnnl=1&oref=slogin&adxnnlx=1190416845-RqzMjP1uACfDN%2BkQ%2B%2FGi0w.

22_ "About." Overseas Security Advisory Council (OSAC). https://www.osac.gov/Pages/AboutUs.aspx. Accessed 20 August, 2017.

23_ Johnston, Judith Meister, and Rob Johnston. "Testing the Intelligence Cycle Through Systems Modeling and Simulation." In *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*, 45-57. Washington, DC: Central Intelligence Agency, 2005.

24_ Stephen Marrin "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis, Intelligence and National Security," *Journal of Intelligence and National Security,* Vol.26:2-3 (2011), 192

25_ James A. Barry, Jack Davis, David D. Gries and Joseph Sullivan. "A progress Report: Bridging the Intelligence-Policy Divide," p. 8 Available at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol37no3/pdf/v37i3a02p.pdf. Accessed on 11/9/2017.

26_ This is based on personal experience and interaction with the United States Government and Private Companies.

27_ Jack Davis, "The Kent-Kendall Debate of 1949,"p. 92, found at: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol35no2/pdf/v35i2a06p.pdf, accessed on: 11/9/2017

28_ President's News Conference of April 21, 1961 (139)," Public Papers of the Presidents: John F. Kennedy, 1961.

Collection Planning
A Cross-Domain Approach

Jorhena Thomas[i]

Abstract

In the coming years, the new generations of intelligence professionals will become more resourceful and multi-dimensional in their collection and analysis work, and by necessity, start to more routinely incorporate non-government and non-traditional resources into their collection strategies. Cross-domain collection planning is about more than embracing open sources, although that is a key part of it. It is also an adjustment in analytic thinking toward a "yes, and" mentality. There are three primary reasons that this approach serves the analytic process well: 1) the analyst will get a broader array of intelligence to assess, or at least increase the chances of doing so; 2) the thought processes required to develop a collection plan in this way provides a rich opportunity to identify new "unknowns"; and 3) this type of collection planning provides a built-in contingency plan by ensuring multiple avenues of collection in case others become unavailable. Two models that jointly complement the cross-domain collection approach are the problem definition model (PDM) and the target network model (TNM). While problem definition focuses on methodically narrowing and refining the scope of inquiry, and cross-domain collection planning meticulously explores all avenues of collection, target network modeling visually organizes and links the incoming intelligence. Part One of the article focuses on how collection planning can evolve to be broader in its scope, and considers important implications for the analytic process. Part Two explores the five key steps to methodically preparing a cross-domain collection plan.

***Keywords*:** cross-domain, Problem Definition Model (PDM), Target Network Model (TNM), asset identification, engagement plan.

---

i Georgetown University. Email: jt1191@georgetown.edu.

Introduction

"Plans are of little importance, but planning is essential."
— Winston Churchill

This article highlights the value of inclusive, holistic, and cross-domain intelligence collection planning, and its implications for the wider analytic process.[ii] The approach is rooted in the need to fill a gap both in the scholarship debate on intelligence tradecraft and the intelligence cycle, and the toolbox of mechanisms within the reach of intelligence professionals[iii]. More specifically, this approach addresses a trend that, although not new, could become one of the new working routines for future generations of intelligence professionals: developing role versatility and incorporating non-government and non-traditional resources into their integrated collection-analysis strategies.

Although time and circumstances do not always allow, when they do nevertheless, developing a solid intelligence collection plan (ICP) is a must for any successful analytic endeavor. Thoughtful collection planning is not a static checkbox within the intelligence cycle, but is a fluid process that requires a great deal of analysis – even before arriving at the formal analysis part of the cycle. More **precisely, the quality of analytic thought that goes into collection planning can make the difference between strong analytic products that are useful and actionable, and weak analytic products that are not of much value to the customer.**

The content discussed herein seeks to provide practical considerations on how the new generations of intelligence professionals can leverage cross-domain collection planning to improve and facilitate their work. This discussion is based on a multidimensional approach to the collection-analysis binomial and the belief that, as Retired United States Army General Stanley McChrystal noted while leading the U. S. Joint Special Operations Command: "The more people you shared your problem with, the better you'd do in solving it."[1]

This article addresses collection planning in broad terms. The content is meant to encourage expansive thinking to provide answers to how, in general, intelligence professionals from all sectors can approach the task of developing systematic collection plans that leverage the wide array of intelligence available and feed into

---

ii In the context of collection planning, the term "cross-domain" is used throughout this discussion as a collective term that means strategically looking for intelligence outside of the realm in which we are working, and engaging with non-traditional sources of intelligence. It always involves being inclusive and holistic; "inclusive" refers to being open to other types of collection sources than those that we generally rely on, while "holistic" expresses a deliberate consideration of all angles of the intelligence requirements, and where they intersect, when deciding on where to collect.

iii The term "intelligence professional" is used throughout this article to include intelligence managers, analysts, collectors, and any other roles involved in the collection planning process. The term "analyst" is used when the content addresses issues particularly relevant to the analyst role.

thoughtful analysis. The collection planning ideas that are to be analyzed in the next pages can be applied to all sectors of intelligence, but are primarily geared toward government intelligence efforts. Because intelligence professionals in the public sector are often trained to use a closed set of collection resources that are already trusted and vetted (such as other government agency information), they run the risk of excluding many other potentially useful collection resources outside of their domain. However, the information provided and discussed herein can be applied to private sector intelligence professionals as well.

Furthermore, it is important to note that cross-domain collection planning can be applied in both strategic and tactical intelligence work. At the strategic level, it can help to chart out a clear path for an investigation or broad intelligence initiative. At the tactical level, it can help operators to know which actions to take and which leads to follow. The level of planning will reflect the overall goal, whether it be strategic or tactical, but the comprehensive thought processes and the value of exploring across domains are the same regardless.

Collection as an integrated part of the analytic process (in contrast with the traditional, linear view of the intelligence cycle) has been ignored and not properly addressed within academic and practitioners' research. Hence, building on the existing literature on the collection-analysis relation and the information management as part of the intelligence cycle, this article will illustrate the importance of a more insightful coordination between intelligence collection and analysis in a two-stage process. First, it will focus on how collection planning can evolve to be broader in its scope, and considers important implications for the analytic process. Second, it will explore five key steps to methodically preparing a cross-domain collection plan that can enhance the analytic process.

A Shift in Thought

> *"The ultimate goal…is to produce all-source intelligence, or fusion intelligence– in other words, intel based on as many collection sources as possible to compensate for the shortcomings on each and to profit from their combined strength."*
>
> — Mark Lowenthal

Intelligence is the best-disguised content in the world, and much valuable intelligence can be found in open sources by engaging with the right collectors. Unfortunately, we, intelligence professionals, often shun what is free and unclassified, and instead place undue weight on intelligence collected by secret means. Mark Lowenthal provides a discerning explanation for why we often discount open source intelligence (OSINT): "Some intelligence professionals

have mistakenly equated the degree of difficulty involved in obtaining information with its ultimate value to analysts and policy makers."[2]

Compared to traditional processes, cross-domain collection planning emphasizes the incorporation of a wide range of resources into intelligence gathering efforts, as wide a range as possible for the given target of collection. Collection planning, as defined by the US Marine Corps, represents a continuous process that coordinates and integrates the efforts of all collection assets and resources[iv]. For this approach to collection planning to gain traction, however, a more intentional effort needs to be placed on educating and training analytic thinkers to appreciate and seek out unique and valuable intelligence available in open sources. Much more than surfing the Internet or reading scholarly papers, knowing how to effectively identify, exploit, and leverage unclassified sources of intelligence from other fields is an advantageous skill set.

Lessons from recent history tell us that open sources can provide uncomplicated and inexpensive access to valuable information. The United States Intelligence Community's years-long work to understand al-Qaeda is an excellent example; al-Qaeda provided a wealth of public information about its intentions, targets, and motivations[3]. Moreover, there are far more sources of OSINT than there are for any of the other collection disciplines. Quantity certainly does not equal quality, but a shift in mindset toward creatively exploring OSINT resources early in the collection process would prove useful to both analysts and collectors.[4]

Although, cross-domain collection planning is about more than embracing OSINT, that is a key part of it. It is also a modification in analytic thinking toward a "yes, and" mentality. The concept of the "yes, and" mentality is this: instead of saying "no" to an idea that seems too out of the box, the method involves agreeing with it and adding to it. Obviously, analysts and collectors cannot say yes to every idea that arises, but they can pause and consider what possibilities are there, especially in the collection planning process.

The "yes, and" way of thinking has been adopted from the improvisational comedy world to education, business, analysis, and other professions as a technique to foster openness to new or non-traditional ideas.[5] In relation to collection planning, which often relegates itself to certain parameters, "yes, and" thinking can be a powerful tool to help guard against common analytic traps such as cognitive bias, anchoring, and mirror-imaging. For example, a law enforcement analyst in the United States developing a collection plan against human trafficking in a certain region might routinely include federal government agencies (Federal Bureau of Investigation, Customs and Border Patrol, Immigration and Customs Enforcement,); state and local law enforcement-affiliated organizations (highway patrol, municipal police,

iv US Marine Corps, MAGTF Intelligence Collection, 2004. Available online at http://www.marines.mil/Portals/59/Publications/MCWP%202-2%20MAGTF%20Intelligence%20Collection.pdf.

High Intensity Drug Trafficking Areas (HIDTA), local fusion center); and maybe a local university with a strong criminal justice program, for good measure. Taking a cross-domain approach and using the "yes…and" mentality, the analyst might consider the array of other entities that could feed collection, such as other federal agencies that are outside of the law enforcement business (such as the Treasury Department), community organizations that work with domestic violence victims, local hospitals, NGOs in neighboring countries that track trafficking data, neighboring government law enforcement liaison personnel, Organization of American States - Secretariat for Multidimensional Security, local emergency services departments, think tanks, academics, subject matter experts, research centers, local online advertising sites, social media, and investigative journalists/media outlets, to name a few. The analyst might also engage with the appropriate analysts in certain intelligence agencies to determine if they have seen overlap between human trafficking and national security issues, and with certain commercial industry contacts to explore how their encrypted messaging applications can be exploited by traffickers seeking to evade detection. This is a basic example of how a simple adjustment in thinking can enhance the collection planning process. By opening one's mind to wider possibilities, and looking beyond the expected sources of intelligence, the analyst can significantly increase the number and breadth of collection resources to leverage.

Furthermore, aside from the benefits of broadening the scope of the collection planning process, the cross-domain approach also has positive implications for the analytic process. There are three primary reasons that cross-domain collection planning serves the analytic process well:

1) **The analyst will get a broader array of intelligence to assess, or at least increase the chances of doing so.** There is always the perceived problem of too much data (too many dots to connect)[6], but broader collection does not equal over-collection. Cross-domain collection planning is not just casting a wider net; it is casting more nets in strategic places. Using the human trafficking example above, the additional entities identified by the hypothetical analyst are not shots in the dark; they are based on a strategic assessment of where potential intelligence could be gathered. The decision to engage with such a broad array of entities was a systematic one, based on a keen understanding of the information sought and an appreciation for what other domains could offer. Intelligence analysis in some ways is a misnomer. It has always been a profession of both analysis and synthesis – a continual process of breaking down complex issues and piecing them together with additional information and insight. Incorporating new sources of collection into this process has the potential to complicate the intelligence professional's work by

providing more information to evaluate. However, for the reasons stated above, the potential benefits far outweigh potential complications.

2) **The cognitive processes required to develop a collection plan in this way provides a rich opportunity to identify new "unknowns"** (new problems, issues, targets, or threats that should be explored) **and to fully understand the current "knowns"** (that is, to have a fuller picture of the requirements already being collected against)**.** Incorporating new and non-traditional sources of intelligence into a collection plan brings new angles to light that may not otherwise have been explored. This also highlights the inherent value in cross-domain interaction; when sectors can gain new insight, perspective, and information from one another, there is mutual benefit in their resulting analyses. Sticking with the human trafficking scenario, the analyst might uncover a dangerous health epidemic circulating among trafficking victims that is slowly spreading to the general population due to their forced prostitution activities. This would be a significant "unknown unknown", as the analyst whose primary focus in trafficking might not even consider related public health impacts. On the other side, those health professionals with whom the analyst engaged will have learned about the trafficking rings and can incorporate this information into their mitigation strategies for containing the epidemic. There is often mutual benefit of this nature to cross-domain collaboration.

3) **This type of collection planning provides a built in contingency plan.** If for some reason a primary source of intelligence dries up or is unavailable, it is useful to have others. Analysis that relies on too few collection sources runs the risk of coming up empty. Again, using the trafficking example, we see that the variety of collection entities listed in the process of cross-domain collection planning is sufficiently broad that should one or two unexpectedly become inaccessible, there is a high likelihood that the other collection sources can provide a well-rounded picture nonetheless.

In their seminal text, *Target-Centric Network Modeling*[7], Clark and Mitchell outline two models that best complement the cross-domain collection approach: **the Problem Definition Model and the Target Network Model**. Their names may sound daunting, but they are simple concepts. One might argue that they are too simple, and are therefore overlooked in the rush to collect intelligence that supports pre-conceived conclusions. However, when they are employed with cross-domain collection planning, they together provide a systematic process that enhances collection and analytic efforts.

1. The Problem Definition Model

The problem definition model (PDM) illustrates a problem[v] broken down to its core elements. Its purpose is to help intelligence customers, managers, collectors, analysts, and others involved in the intelligence process to thoroughly understand a problem at its core, and tailor collection planning to those specific elements. Rather than "shooting in the dark" at a large and unwieldy target, the PDM facilitates rigorous thought from which results an organized starting point for collection planning. Depending on the complexity of the problem at hand, some PDMs will result in the production of multiple collection plans that are specific to a particular element of the problem. PDMs come in a variety of shapes. *Figure 1* is a common one; it is based on a gray arms transfer case study explored by Clark and Mitchell.[8]

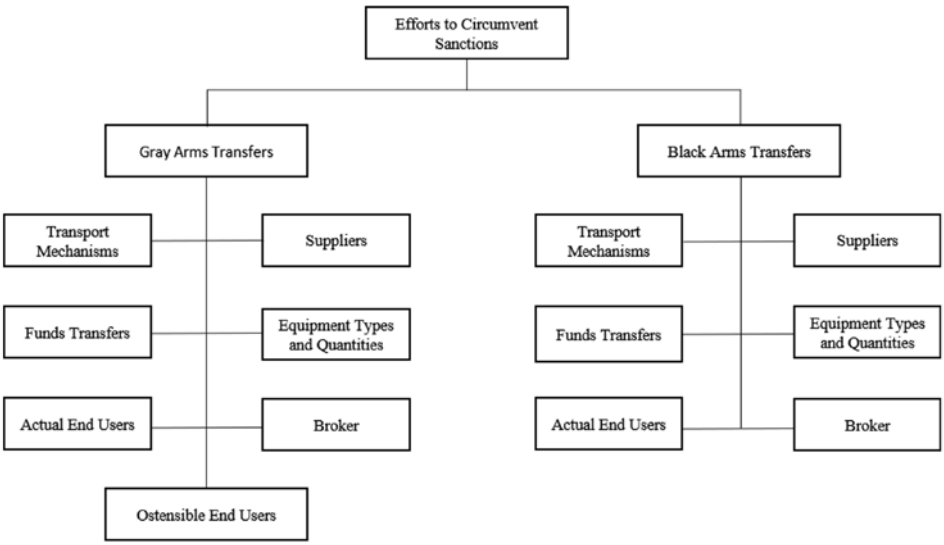


Figure 1: Example of a problem definition model, wherein the uppermost box ("Efforts to Circumvent Sanctions") represents the broad problem set and the cascading boxes represent core elements of the problem. Source: Clark and Mitchell, *Target-Centric Network Modeling,* Figure 2.6, Circumventing Sanctions PDM 1.1,16.

2. The Target Network Model

The target network model (TNM) is a way of organizing collected intelligence that encourages - and even thrives on - input from a wide variety of sources. The TNM is effective for looking at networked problems (as most problems are) and for linking the disparate sets of raw intelligence that analysts must piece together and assess – *Figure 2*. It is important to make the distinction

v The term "problem" is used to collectively refer to an intelligence problem, issue, target, or threat.

between a well-structured TNM and a general link chart. TNMs have a clear focus on the defined problem, and orient collected intelligence toward that focus. Like PDMs, TNMs can take different shapes and formats. They are superior tools for parsing, evaluating, and visualizing gaps in information. TNMs are by nature flexible and easily-modified. Just as the analytic process is fluid and can change direction quickly, so can the TNM adapt to new intelligence and changes in analytic judgements. Further, TNMs lend themselves exceptionally well to cross-domain collection, as they allow the analyst to consider intelligence that may diverge from other pieces of intelligence; annotate and weigh the sources of intelligence; annotate tenuous or unsubstantiated information; place levels of confidence on pieces of information; and notice patterns in reporting/collection. *Figure 2*, below, is also based on Clark and Mitchell's gray arms transfer case study.[9] It uses the "Broker" node as a central point of collection.

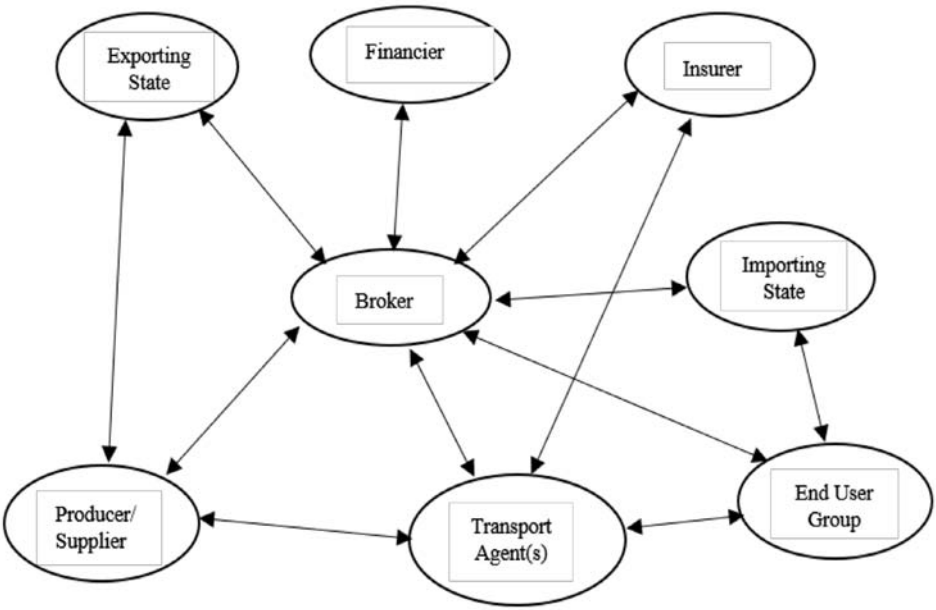


Figure 2: Example of a target network model, wherein the center area ("Broker") represents the primary node and the branches represent related nodes based on collected intelligence. Source: Clark and Mitchell, *Target-Centric Network Modeling,* Figure 2.9, Generic Arms Transfer Network Model, 21.

Cross-domain collection planning plays a key role in the process between defining the problem and charting the incoming intelligence. While problem definition focuses on methodically narrowing and refining the scope(s) of inquiry, and

target network modeling visually organizes and links the incoming intelligence, cross-domain collection planning meticulously explores all inclusive, holistic avenues of collection.

Problem Definition Model (PDM)	Cross-Domain Collection Plan	Target Network Model (TNM)
Visual representation of central elements of given problem. Establishes shared situational awareness and aids in thorough understanding of core issues.	Inclusive, holistic plan to gather as much useful intelligence from as wide a variety of sources as feasible. Serves as key step between PDM and TNM.	Visual representation of collected intelligence. Ideal for charting and evaluating raw intelligence from a wide variety of sources.

Figure 3: Cross-domain collection planning is based on the PDM and drives the intelligence gathering that populates the TNM.

Pulling It All Together

> *"For the intelligence analyst, critical thinking requires…a predisposition toward inquisitiveness, an almost limitless curiosity about any and all subjects or processes. Curious minds tend to stay open to possibilities."*
> **—** *Robert M. Clark and William L. Mitchell*

The considerations provided in the first part of the article have been consolidated into the following five steps to guide the intelligence professional looking to employ this approach into future collection planning efforts.

1. The first step to be considered is **Problem Definition**. This process requires the identification and definition of the problem/target/topic/issue/threat as specifically as possible. The problem is usually embedded in a question issued by the customer of the intelligence product and addressed to the analyst: "What am I ultimately trying to find out?" or "What are my operators trying to accomplish?" or "What information is my CEO trying to uncover?" It is important for the analyst(s) to be keenly aware that the questions asked by customers may not be what they actually need or want. As Clark and Mitchell

advised, "never accept the problem definition stated by the customer as is."[10] As a result, it is necessary not just to ask questions, but to restate them and pay attention to what is not being said to get down to the core of what is needed. When possible, using a visual problem definition model may help find the core elements of a problem.[11]

2. After establishing as clear as possible what the problem to be addressed is, the intelligence professional needs to craft a specific and realistic set of priority intelligence requirements that stands as the second step, **Requirements Development.** Efficient collection planning hangs on a clear problem definition and well-crafted intelligence requirements. When crafting priority requirements, the intelligence professional needs to phrase them as questions and narrow them as specifically as possible. For increasing accuracy, priority requirements must be continually compared to the problem definition to ensure that they are aligned. Each requirement should address one issue only, as combining issues within one requirement can muddle the analysis process.

3. The next step is **Asset Identification**, which consists of determining where to get the specific information needed. An asset is any entity or resource that may have intelligence useful to satisfy requirements. To this end, a strong plan explores all collection possibilities, is based on all-source collection, and includes a range of agencies, organizations, and companies **(in accordance with applicable laws, and as appropriate**)

[vi]. Each sector of activity has its own specialized entities and assets that can be engaged in the collection process and therefore provide different pieces of the puzzle:

- National Security Assets: national/ federal government and military agencies and commands (intelligence-centric and otherwise); intelligence branches of agencies not part of the intelligence community
- Law Enforcement Assets: national, regional, provincial, state, and local law enforcement services; law enforcement arm of many government agencies (usually its own branch with unique access to information sources); high-intensity drug trafficking areas (HIDTA); INTERPOL and other international law enforcement cooperation organizations
- Private Sector Assets: academic institutions and experts; financial institutions; community centers; research centers; open sources/ social media; industry resources; media outlets; think tanks; non-governmental organizations; technology companies; trade shows; subscription satellite imagery; congressional testimony/reports

vi The United States, for example, has a complex system of laws and guidelines that limit collection of certain information by certain agencies; limit the manner in which some collection can occur; and rigorously protect privacy, civil rights, and civil liberties.

- Other/Specialty Types of Assets: international organizations; foreign government partners; fusion centers; information-sharing and analysis centers (ISACs); FOIA-requested information[12]; regional military and defense universities; court records; regulatory bodies

When thinking through the assets, the intelligence professional should consider:

- The type of intelligence each could provide, along with limitations on collection in terms of the sensitivity of the work; applicable laws; feasibility; public perception; timing; privacy concerns; and other potential hindrances.
- How they would get it (that is, what collection discipline(s) they would use – GEOINT, HUMINT, MASINT, OSINT, SIGINT). This is important to consider because the method of collection can place limits on how the resulting analyses are used and shared.
- How you would get it from them (that is, your engagement plan, which is addressed in Step 4.).

4. In order to increase the efficiency of the collection process in terms of relevant inputs, the **Engagement Plan** becomes a must. This forth step consists of determining how to submit requests to your assets. Engagement plans can include both formal and informal interaction with assets, such as: informal direct contact (analyst-to-analyst or analyst-to-collector contact), formal requests for information (RFIs), structured joint operations, formal and informal consultations, formal contact via established intermediaries/liaisons. Engaging with the right department/unit within an agency/organization is crucial; just as intelligence requirements work best when they are as specific as possible, so does the engagement plan. The engagement plan for each agency/organization should be appropriate for the way it does business. This is particularly important to keep in mind in cross-domain communications, in which unfamiliar policies, communications platforms, organizational cultures, jargon, and other factors come into play.

Intelligence Collection Plan Checklist

- ✓ **1**. Well-defined problem
- ✓ **2**. Specific and realistic set of priority intelligence requirements
- ✓ **3**. Identified entities (agencies and organizations) with access to the intelligence to satisfy the requirements
- ✓ **4**. Practical and tailored engagement plan for each entity
- ✓ **5**. Target network model or other model in which to organize and link collected intelligence
- ✓ **6**. For collection that may lead to legal process/court: parallel construction plan

5. Target Network Modeling represents the fifth step and implies the organization and linking of collected intelligence. The use of a target network model (whatever form fits the need) keeps raw intelligence organized and gives it meaning in relation to other pieces of intelligence. The modeling based on cross-domain collection facilitates pattern observation and gap identification, and can lead to otherwise unexplored avenues of inquiry that are critical to the analysis ("unknown unknowns"). However, it must be well understood that the model should be treated as a means to an end, and not the end itself.[13]

For intelligence professionals in law enforcement, there is an extra challenge in collection planning. The ability to collect intelligence (evidence) to build a case suitable for the legal process at times requires two collection plans – one to serve as a broad lead-generator and one appropriate for the legal process. A particularly poignant example is that of a terrorism investigation. Evidence is likely to include both closed (classified) intelligence as well as open source intelligence. While the classified intelligence can't be used in open court, it can be used to lead to equally valuable evidence that can. Therefore, it is prudent to have two concurrent collection plans to meet this need, a process called "parallel construction". An entire article can be written on this topic, but it suffices to mention here that the cross-domain collection planning process lends itself particularly well for these types of circumstances.

Conclusion

"One must always proceed with method"
— Hercule Poirot

Cross-domain collection planning is a method of gathering intelligence that is inclusive, holistic, and open to information from an array of inter-disciplinary resources that complement one another and lead to more robust analytic processes. More than an approach for collection, however, it is a way of thinking systematically and strategically about what is needed and who can provide it. It is instructive for training intelligence professionals how to think creatively and non-traditionally about their intelligence needs. In additional to fostering creativity, it also leads to new possible collection avenues and the identification of new "unknowns".

While embracing a collaborative and open mindset in collection planning has a wealth of benefits, there are some pitfalls that the intelligence professional should be aware of, such as maintaining confidentiality with sensitive information; navigating political, organizational, and cultural barriers; managing disparities or conflicts in the intelligence collected; handling too much or too little useful intelligence; and assessing the reliability of the intelligence collected.

Nonetheless, the benefits far outweigh the potential pitfalls. When combined with robust problem definition and target network models, and used by skilled intelligence professionals, cross-domain collection planning can have a significant impact on the quality of the analytic process.

Endnotes:

*01_* Dana Priest and William M. Arkin, "'Top Secret America': A look at the military's Joint Special Operations Command", The Washington Post, https://www.washingtonpost.com/world/national-security/top-secret-america-a-look-at-the-militarys-joint-special-operations-command/2011/08/30/gIQAvYuAxJ_story.html?utm_term=.35fa762b716d.

*02_* Mark Lowenthal, *Intelligence: From Secrets to Policy* (Los Angeles: CQ Press, 2017), 150.

*03_* Erik Dahl, *Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013), 132.

*04_* "INTelligence: Open Source Intelligence", Central Intelligence Agency, accessed September 20, 2017, https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

*05_* Bob Kulhan, "Why 'Yes…and' Might Be the Most Valuable Phrase in Business.", Big Think, accessed September 20, 2017, http://bigthink.com/experts-corner/why-yes-and-might-be-the-most-valuable-phrase-in-business.

*06_* Alex Young, "Too Much Information: Ineffective Intelligence Collection", Harvard International Review, http://hir.harvard.edu/article/?a=10382.

*07_* Robert M. Clark and William L. Mitchell, *Target-Centric Network Modeling: Case Studies in Analyzing Complex Intelligence Issues* (Los Angeles: CQ Press, 2016).

*08_* Clark and Mitchell, *Target-Centric Network Modeling*, 16. Used under permission of U.S. copyright law fair use standards.

*09_* Clark and Mitchell, *Target-Centric Network Modeling*, 21. Used under permission of U.S. copyright law fair use standards.

*10_* Clark and Mitchell, *Target-Centric Network Modeling*, 28.

*11_* Clark and Mitchell, *Target-Centric Network Modeling,* 4.

*12_* T.J. Waters, *Hyperformance: Using Competitive Intelligence for Better Strategy and Execution* (San Francisco: Jossey-Bass Press, 2010), 65-71.

*13_* Clark and Mitchell, *Target-Centric Network Modeling,* 22.

Scenario Analysis: Combining Intelligence Analysis Methods

Humberto Hinestrosa[i*]

Abstract

Generating Strategic Scenarios has been evolving through time since WWII and were used with success by Shell and other organisations to foresee major events between the 70s and the 90s. Likewise, Governments for the last ten to twenty years have been using scenarios' techniques to study what they consider key strategic drivers and trends as an effort to enrich intelligence analysis. The scenarios technique is a very complex tool and process that has shown that it is possible to bridge the gap between national security and the private sector. When used properly, it considerably improves intelligence analysis and the organisation mind-set, thus, adding significant value to intelligence analysis. Scenarios methodology, by design, encourages critical thinking and includes the use of analysis methods, dealing with most of the traditional intelligence analysis cognitive problems inherent to the human condition. Moreover, Scenario Analysis studies the driving forces, critical uncertainties, and how they may shape the future. This paper seeks to highlight the value of scenarios for intelligence analysis methodology. In addition, this paper aims to assess in more detail to what extent scenarios may contribute to the improvement of strategic intelligence in both, the private and national security sectors.

***Keywords*:** Scenarios, Structured Analytic Techniques (SATs), intelligence analysis, cognitive biases, analysis methodology

i * Independent defence and security consultant with experience in the public and private sector. Email: hinestrosa@gmail.com

Introduction

Scenario Analysis is a complex tool that is currently used in government and in business. This tool, when well-used, has the potential to improve the intelligence analysis process and to add significant value to the final intelligence product. Although scenarios are currently developed in the Anglosphere as an analytical tool to support long-term decisions, the literature has not yet explored its utilisation as a process at the strategic level. This paper aims at exploring the value and the limitations of scenario generation to intelligence analysis by providing a description of the process and how its methodology makes use of different analytic techniques to reach a final product.

Most of the authors referenced throughout this paper belong to the group that has contributed to the development of the scenario methodology, and the 'futures' discipline. Amongst them are the prominent futurists Herman Kahn, Pierre Wack and Peter Schwartz. And most of the current well-known scenarios professionals and academics Professor Thomas Chermack and Kees Van der Heijeden It is worth noting that Wack, Schwartz and Van der Heijeden worked for Dutch Shell, developing the scenarios techniques that later would become part of the Intelligence Analysis Techniques literature.

The referred scenarios will be studied in a different perspective, as a macro or strategic tool rather than a device as in Central Intelligence Agency's (CIA) Tradecraft Review[1] or Heuer-Pherson's Structured Analytic Techniques for Intelligence Analysis (SATs)[2] work. It is important to highlight that this article will not elaborate any further than the process and analytical aspect of scenarios and their value-relation to the intelligence analysis field. However, it is worth highlighting that the value and use of Scenario Analysis expands beyond the analytical realm; as it will be discussed, it is also a tool to improve organisational aspects and to bridge the gap between analysts, managers and policymakers.

Scenarios: Background and Current Use

Scenarios have their origins during the Second World War as a planning method for alternative military strategies.[3] The formalisation of scenarios and futurology can be traced back to Herman Kahn, prominent futurist who formed part of the U.S. Air Force efforts against Nazi Germany. Kahn was also a member of the RAND Corporation and the founder of the non-profit think tank Hudson Institute, based in Washington, D.C. At the time, the RAND Corporation was researching new forms of weapons technology, and Kahn was leading the effort and pioneering the technique he named 'future-now.' Under his direction, the Hudson Institute focused on stories about the future to aid people to consider the unthinkable.[4] His interest after the war, apart from nuclear power use, was futurology, focusing his efforts on social and economic issues. Herman Kahn

defines scenarios as "a tool for business prognostication," and his approach can be described as imaginative and detailed reports about the future as if they were written by people from the future. Although he was a pioneer at that time, his viewpoint was leading the trends in corporate planning; but clearly, his view was—in retrospect—precarious. He imagined the future as already occurring.

Years down the line, in 1970, scenarios changed with the work of Pierre Wack who was part of the Group Planning department at Royal Dutch/Shell offices in London. At the time, the Group Planning team was looking for events that may affect the oil price in the future. Wack considered that scenarios, to be truly effective, must change managers' conception of reality, that is, to have them think beyond outside of the box. He encouraged managers to imagine all decisions they might take in the future.[5] In the early 1970s, Wack's team developed two possible scenarios about oil prices, and later in 1973 when the Yom Kippur War crisis occurred, they were able to adapt successfully to the changes brought by this conflict, thus validating the effectiveness of their work. Because Wack and his team were able to see beyond the present situation, Shell was the only company at the time to efficiently and effectively respond and adjust when facing to oil crisis. At this stage, it was clear that the main concern for the planning team was the decision- makers' mind-set.

In 1985, Wack wrote 'The Gentle Art of Re-perceiving' which became a significant contribution to scenario planning literature. To encapsulate the idea of Wack's re-perceiving, in his work "The Art of the Long View," Peter Schwartz stated:

> *"To be able to operate in an uncertain world, people need to be able to re-perceive—to question their assumptions about the way the world works, so that they could see the world clearly. The purpose of scenarios is to help yourself to change your view of reality—to match it up more closely with reality as it is, and reality as is it going to be."*[6]

Peter Schwartz explains that Wack's efforts were not solely focused on predicting the future, instead, he wanted to explore people's mind-sets and their underlying forces. Peter Schwartz used Wack's ideas in the aforementioned work "The Art of the Long View" to develop his own view of the scenario methodology. Peter Schwartz was part of SRI International (formerly known as the Stanford Research Institute) in 1975 and although he initially followed Herman Kahn's ideas, he later adhered to Pierre Wack's scenario conceptions. In 1985, he joined the Planning Group at Royal Dutch/Shell, replacing Pierre Wack, who was retiring. Schwartz remained at the company for five years working as the head of Scenario Planning, and later founded Global Business Network (GBN).[7]

In 'The Art of the Long View,' Schwartz offered a more conceptual approach on

scenario planning. His book describes the basic approach used by GBN, and is considered to be a fundamental contribution to the scenario planning literature.[8] Schwartz's work later became relevant to the intelligence analysis tradecraft as shown by the main source of reference for scenario techniques described in the CIA Tradecraft Review and the Heuer-Pherson's 'Structured Analytic Techniques'.[9] It is worth noting that the CIA Tradecraft Review dedicates a mere three pages to the alternative futures technique, a very simplified version of scenario analysis. The CIA publication explains the basics on how to cross the forces and develop those alternative futures. The Tradecraft Review also acknowledges that this tool should be used for situations with a high degree of uncertainty and should be assisted by an expert in such techniques.[10]

Similarly, Heuer and Pherson, in their book *Structured Analytic Techniques for Intelligence Analysis*, also show interest in scenarios and dedicate a chapter to elaborate more on when and how to use such technique. They provide the reader with a shorter version of Peter Schwartz's scenarios, but still recommending expert advice. Heuer and Pherson make three versions based on the number of analysts involved, number of forces involved and the number of the resultant scenarios; those three versions are: Simple Scenario, Multiple Scenarios and Alternative Future Scenarios.[11] Despite adding more detail and adapting the technique, this attempt remains a simple approach to what the scenario process actually involves. Although it [scenario analysis] is presented as an analytic device and an individual tool that, as such, may not bring entire valuable strategic outcomes, Heuer and Pherson make a remarkable contribution for analysts by reaching less-complex scenario plots more efficiently and by introducing some basic guidance about these techniques serving more simple analytical tasks.

Scenarios have also been included in the set of tools and have been used by the CIA, the National Reconnaissance Office (NRO) and the National Intelligence Council (NIC) – all three which have a Long Range Analysis Unit.[12] Similarly, 'Horizon Scanning' became the British version of scenarios, and has been used in various departments since late 1990s. The Strategic Horizons Unit (SHU) at the Cabinet Office was created in 2008, and the Developments, Concepts and Doctrine Centre (DCDC) are primary users and producers of scenario-based products.[13] The UK government, through the DCDC, periodically releases a document named Global Strategic Trends, which contains a detailed analysis of the future strategic context within the national security perspective. This document covers trends, analyses of alternative futures, drivers, risks and implications out to thirty years ahead.[14] Its counterpart in the US, the NIC issues the Global Trends, and the NRO publishes the Proteus Project, and like the British version, they are released periodically. It is worth highlighting that Global Trends identifies key trends, drivers and strategy to foresee strategic opportunities for the future policymakers within a long-term timeframe.[15] The methodology described within both publications, mention the use of subject

matter experts, think tanks and scholars to identify the key forces that may influence the future. The UK version specifies that it is based on driver and trend analysis, while the US version specifies that it relies on scenarios to indicate the drivers.[16] These elements will be explained in more detail later.

Structuring Scenarios: Opening the Door for Structured Analytic Techniques

With regards to methodology and how scenarios are generated, one should first note that forecasting must be distinguished from scenarios. As Kees Van der Heijden asserted,

> *"...forecasting assumes that it is possible to predict the future, on the basis of what we have called a 'variance theory,' [...] consistent and ongoing correlations between variables."*[17]

In other words, forecasting might have a rationalistic approach[ii] based on the existence of one single answer to the matter, which means it is rather simplistic. Contrarily, for Van der Heijden, scenarios are based on the fact that "the future is not predictable, it contains irreducible uncertainty." But behind events there are causes that can be studied and structured in order to develop a theory about 'why things happen.'[18] Moreover, according to how Schwartz viewed and conceived his idea, scenarios were the source method in which intelligence analysis methodologists based their scenario analysis techniques.[19] According to Schwartz, in order to build scenarios there are some steps that must be followed: (i) isolating the decision after determining the needs; (ii) identifying the key factors that will affect the decision; (iii) developing the plot and (iv) rehearsing the implications.[20]

First, uncovering and isolating the decision in this context means to identify the focal issue; thus, scenarios should be built around a central concern.[21] The decision must become a conscious process and Schwartz argues that to reach that point of consciousness, decision mind-sets must be broken because they keep us from seeing the appropriate and relevant questions. The belief that the future is going to be similar to the present must be challenged, and the planner must be prepared to recognize the change when it happens. In other words, the planner, analyst and decision-maker must ask the right question and look into the right direction. Therefore, the planner/analyst

---

ii The rationalistic approach would be defined by the use of reason and a logical structure. According to the Encylopaedia Britannica "Rationalism, in Western philosophy, the view that regards reason as the chief source and test of knowledge. Holding that reality itself has an inherently logical structure, the rationalist asserts that a class of truths exists that the intellect can grasp directly. […] Rationalism has long been the rival of empiricism, the doctrine that all knowledge comes from, and must be tested by, sense experience."
"Rationalism." Encyclopedia Britannica. N.p., 2017. Web. 2 Dec. 2017.

must look back at the organisation's assumptions and perceptions; this is a process of self-reflection, understanding biases (personal and organisational), that matters to the analyst and the organisation in order to perceive where to focus the attention. Broader and specific questions matter, and by dismissing any of these, the analyst may miss something important.[22] During and after the process of finding the right questions and sharpening the decisions, the collection of information takes place. This is a dynamic procedure. The gathering process is used to disconfirm information as collection may challenge current or past assumptions and may sharpen the ability to perceive relevant information. The flexibility of perspective is necessary based on the assumption that the collector may gather what he thinks he needs to know.[23]

Second, by identifying the key factors, Schwartz explains that the issues affecting the decision must be clearly identified and through them, one can begin to explore the driving forces implying additional methodological steps. According to Schwartz, driving forces are "the forces that influence the outcome of events."[24] For Kees Van der Heijden these are "those fundamental forces that bring about change or movement in the patterns and trends that we identify as unpinning events in the world."[25] Furthermore, Van der Heijden explains that "driving force[s] has relatively high level of explanatory power in relation to the situation being looked at."[26] Identifying driving forces is not a simple process; it involves research and the use of structured analysis to recognize and understand them. In order to do so, a deep research on diversity of disciplines—mostly social sciences—could be conducted; these may include economic, political, environmental, social and technological variables as the main categories.

A classical approach is to follow the STEEP headings model as a research checklist to scan external factors and developments.[27] It stands for Social, Technological, Economical, Environmental, and Political, but the analyst may consider many other variants (e.g. PEST, STEMPLES, STEEPLED) that may include other factors such as military, security, demographic, religious or legal. Following the identification of drivers, 'predetermined elements' and 'critical uncertainties' must be uncovered for each driver as well.

On the one hand, predetermined elements according to Wack are those "that have already occurred […] or almost certainly will occur, […] but whose consequences have not yet unfolded."[28] Identifying them is essential and will be critical for scenario building as there are always predetermined elements in the future.[29] Scenarios should seek the structure of the events in the environment and in the same way; those predetermined elements will be constant along all scenarios.[30] In other words, predetermined elements will constitute 'what we know.' For instance, demographics are the most common and easy way to find predetermined elements. It is certain and has been accurately traced over the years that this element will be a constant in the future. After a 'baby boom,' one should expect that young population would grow after the years; which brings new problems, new needs and the emergence of economic changes. On

the other hand, the critical uncertainties are intimately connected with driving forces and associated to timing and intensity of change of those driving forces.[31] Different interpretations of such uncertainties may provoke scenarios to differ, which means the analyst's insight and perception will play a significant role.[32] In this case, critical uncertainties become 'what we do not know.'

After having the driving forces, predetermined elements and critical uncertainties well identified, the next stage should consist in their classification according to their impact and uncertainty in order to 'plot them.'[33] Then the interacting forces should be evaluated to look at the converging points between them, the forces' interaction may generate different futures and make up unique stories to every future. The key aspect, explains Schwartz, is to look at "…what plots make you do something different…"[34] Some authors, such as Wright, Van der Heijden or even Heuer use matrixes as an aid to cross reference the mentioned forces and develop alternative futures to build a story. However, those stories or alternative futures may only be two or three, "because people's minds can cope with only two or three possibilities, […] on rare occasions you might consider four. At the same time, using more choices will produce a hopeless muddle," explains Schwartz.[35] Furthermore, if too many stories are considered, this could lead to error as too many considerations forces and implications cannot be handled by an individual or even may lead to studying other key issues (or too many unnecessary issues) in detail. Consequently, those plots must be as different from each other as possible, coherent and logical.

The last step is the identification of indicators; these will confirm which plot is unfolding among the possible futures. Indicators are those 'specific signals' that might confirm in advance that the change is approaching.[36] Generally speaking, indicators come form as a list of events generated during the research process that are unique to one specific scenario, but not observable in any other scenarios. For Schwartz, indicators must be as specific as possible, so they are not open to misinterpretations.[37] The diagnosis power of an indicator is key to identify with precision a determined unfolding scenario. However, indicators present in more than one scenario reduce its diagnosis power and therefore, its value as an element of diagnosis. In summary, a good scenario indicator must be observable, valid, reliable, stable and overall, unique.[38] Indicators will let the organisation and the analyst know how to act, what to expect, what events to look at and as a result, will become an essential element to reduce surprise.[39]

Missing to Identify the Communist Collapse: The Private Sector Contribution

The success stories of scenarios building as well as intelligence successes are often not documented, especially because the key methodological details of how organisations and intelligence agencies look into the future are carefully guarded.[40] But in one case, the collapse of communism in the Soviet Union was

the example of excellence that compares scenario performance in contrast to other traditional analytic practices. On the one hand, the CIA is criticised by missing the collapse of the Soviet Union: not being able to anticipate the end of the Cold War, one may argue that it was a surprise or at least that they missed identifying the timing of the events. One of the most high-profile reproaches for this failure came from the New York senator at that time Daniel Moynihan, who was also part of the Senate Committee on Intelligence for many years.[41] Senator Moynihan asked, how did the CIA, which had been following for years in detail all Soviet activity, miss such event? He argued that the information was publicly available, therefore, it was a prediction that anybody, including him, could have done. Moynihan claimed that CIA had a 'myopic' focus on classified information, despite of all available open-source information, which led to the failure to predict the demise of the USSR.

However, Bruce Berkowitz studied in more detail all intelligence estimates at the time and he suggests that the CIA was not as wrong as Senator Moynihan claimed, but still failed to anticipate 'intensity' and 'speed.' Some of the key disagreements among the IC were related to how severe was the crisis and how they would deal with it.[42] As a matter of fact, the CIA warned the government about a weakening of Soviet economy, but was unable to consider the chain of events that ended with the fall of the USSR. They did not understand the impact or the severity of the current events; they though that the Soviet Union would evolve, not collapse. Moreover, President Bush did not give legitimacy to the coup plotters when it happened, based on the assessments that the coup "was not a competent one." US policy evidently was too attached to current intelligence and was lacking of perspective.[43]

On the other hand, in the 1980s, the Troll platform was one of the biggest and most expensive oil & gas projects, and was carried out by Royal Dutch/Shell in the North Sea. This project was a significant investment that would be seriously affected by a sudden fall of world oil prices. To that end, Shell's scenarios team researched what plausibility and what events could cause an oil price change. Those questions led the researchers to study the Arab OPEC countries, and the role of the Soviet Union and its political stability. The question following this was: what might lead the Soviet Union to a dramatic policy change? In a simplistic way, the answer was that the economy was no longer sustainable, it was facing a crisis and the population was not young enough to activate productivity. Therefore, the research team foresaw two possibilities: The USSR would 'muddle through' or will open up. These two scenarios were called 'Incrementalism' and the 'Greening of Russia.'[44] Shell's team considered all political options, like Gorbachev's massive economic and political reforms, declining of tensions with the West, and his role in the government and communist party. Gorbachev's role was an indicator of other primary causes.[45]

Summing up, the CIA and Shell team had access to the same information.

Schwartz asserts that during their presentation to government agencies, the CIA objected their scenarios, claiming that they (Shell) did not have the facts. In fact, the difference in conclusions between CIA and Shell was a matter of asking the right questions. The CIA was trying to consider one single answer; they were being reductionists. Instead, Shell was ready for the change and already understood the current facts and how the future was unfolding.[46]

Assessing Scenarios

As Mark Lowenthal claims, the function of intelligence is to reduce uncertainty, and intelligence analysis has been trying to cope with providing knowledge and the best answer possible.[47] But intelligence, as any process, has its own limitations. The human cognitive process is a predetermined limitation to intelligence analysis and it cannot be eliminated, thus, this condition will be permanent. The improvement efforts in analysis have been directed in part to reducing the effect of this condition by structuring human logics and thinking, in order to reduce failure. Richard Betts explains that the power of knowledge sometimes could be erroneous, irrelevant, or impotent. As a result, knowledge will depend on who has it, how is it used, and how accurate it is. Moreover, the same author also argues that "among the inherent enemies [of intelligence] are the physical limitations of cognitive processes."[48]

Likewise, scenario building is a process that uses more than a single particular technique, and according to Wright, it is a social-reasoning process that shares perceptions.[49] He explains that it is a "systematic way to look into the future, […] focused on perceptions of the casual unfolding events," which means that today's scenarios are no longer speculative as its previous versions.[50] This process has different steps in which all are performed by humans. The approach in its own process is based on dealing with the human condition to produce an outcome associated with the future. In other words, its approach regarding to the cognitive limitation as the starting point is its nature.

Also, when scenarios fail, it is often because most of the time the scenario planners that could not understand the threat, they did not break mind-sets or they did not formulate the right question, failing in a similar way as some intelligence failures found in intelligence literature. For example, anticipating the fall of the Soviet Union.[51] Scenarios, according to Wright, are both an art and a science, and in some perspective limitations from both [art and science] would be present; it provides logical structure and method, but still depends on some intuitive thought.[52] Similarly, estimative intelligence is also an art and a science; so, according to Friedman, it will therefore be imperfect.[53] Consequently, both intelligence and scenarios share the lack of perfection as a limitation. Error is an inherent and unavoidable element.

Another limitation remarked by Wright and Goodwing, is that scenarios do

not estimate probabilities. The multidisciplinary approach, qualitative and quantitative elements involved in the scenario analysis process reduce the quantitative aspect of the scenarios as a final product. However, in the intelligence field this could become an insignificant issue.[54] Probabilities estimation would be more an analyst insight and expert judgement thing instead of an exact estimation with defined mathematical chances of occurrence, as some social sciences disciplines, scenario analysis and estimative intelligence processes for national security.[55]

Unlike most intelligence products, scenarios are long stories and may be not read by busy consumers. However, Thomas Chermack claims that a story is an effective way to provide information, that way the product (particularly the scenario plots) could be remembered easily,[56] although at the end, the effects will depend on the consumer, organisational practices or on the subject of study. It could be inferred that scenarios applied to long range timeframes will be delivered in a longer story, so if a policymaker wants to take a look at the future, he will need to read a long analytic product because the future is far from simple.

At the same time, among other benefits of building scenarios is that they encourage a more systematic thinking by analysts, managers and consumers thus offering better perspectives of the problem. Scenarios also improve communication links and credibility with the policymaker by promoting interaction; and seek to break decision-makers' and managers' mind-sets.[57] It can be argued that scenarios provide a conceptual understanding structure about today's global dynamics and complexities.[58]

The scenario building process provides a proper environment for analysts and policymakers to challenge each other mental models and enhances creativity - both have to think the unthinkable, they have to perceive how the future may look like. In order to do so, they are obligated to use backward logic, understand human motivations, and study in-depth possible implications.[59] These are all practices that help the analytic process to avoid cognitive biases, an inappropriate interpretation of current facts and bounded rationality.[60] Through the process, exogenous and endogenous factors are considered. To get the right perception and to get the right question, not only external factors should be uncovered, but also internal factors such as organisational culture or managers' perceptions matter for scenario analysis. These factors may affect the perceptions of the future and may unveil the own organisation limitations.[61]

Based on a number of publications throughout the US and in the UK it is evident the use of scenarios by the agencies of these governments. These publications use principles and methods explained by Peter Schwartz, and are aimed to identify possible trends and scenarios for the upcoming years, in order to recognise opportunities and threats, becoming a useful reference for other analysts at different levels throughout government administrations. Such works, first, seek to stimulate strategic thinking among analysts and consumers and break their

mental models and blurry pictures of the future, and, in consequence, open their minds to new trends. Second, they uncover with increased accuracy and through profound research, the forces that are driving world events.[62] However, David Brooks critiques this position, arguing that those forces are explained in a simplistic way. He considers that such publications are of a low relevancy to intelligence analysis. In fact, his view could be relatively right, but it depends on how tactical or strategic the analysis is done. The benefit of that work is that analysts do not have to use valuable time in finding and studying driving forces— that step is already completed by the DCDC or by the NIC. And what is guaranteed is that the study of driving forces will be more extensive in a specialized department for scenarios employing time and resources to find the right driving forces, than in a small division lacking resources, specialized personnel and time. The summary of these forces lets the analyst know where to look at, and therefore precious time can be saved. Knowing the forces that drive the current world events is fundamental. Oscar Kaplan explains that when the variables and reasons are known, "then […] predictions are likely to be more accurate." The knowledge will increase if "other variables that condition the strength of the above variables [are known in detail]". [63]

Conclusion

Scenario analysis as a process or particular technique contributes to improve intelligence analysis. It seeks to limit or avoid most of the cognitive problems that may appear in the analytical activity, such as biases or bounded rationality. The scenario building process involves critical thinking, assumptions check, the use of disconfirmatory evidence, and many other methods aimed to increase objectivity. Therefore, one could say that scenario analysis could be a great platform to be implemented, within its own process, it is served by other techniques traditionally designed and used in intelligence analysis, particularly SATs such as Brainstorming, Key Assumptions Check, Indicators, Outside-In Thinking, What If? Analysis, Devil's Advocacy, and Structure Debate just to list a few.

Scenarios by design test, challenge and change mind-sets, they do not only provide analysts with a different perspective, but also encourage the user to find the correct perspective in order to formulate the right questions. For example, in the Soviet collapse case, analysts failed by making the wrong questions.

By running scenario analysis, the analyst is expected to operate in a suitable environment that encourages him or her to think the unthinkable based on rational and plausible elements derived from a structured analytical process. Surprises are most of the time unthinkable and unexpected, but scenarios contribute in reducing uncertainty and therefore, in anticipating surprise. Also, scenarios contribute with the identification and profound study of driving forces, critical uncertainties and predetermined elements. Understanding these

forces and elements would become fundamental for more accurate strategic intelligence products providing a logical approach to understand how the future may unfold; it is one of the most significant contributions to intelligence analysis. When looking to the Global Strategic Trends or Proteus Project publications, it is clear that government agencies use this method for strategic thinking, but when looking at the timing, it could raise the question whether governments are sometimes behind. Unless it remain classified, last scenarios' generation was first used by the private sector since the 1970s.

Another critical value is that scenarios allow the organisation and the decision makers to be ready for the future, to react quickly, to find opportunities and to let them be prepared for an uncertain world. The scenario building process may enrich analysts' knowledge saving valuable time when looking for strategic drivers and critical uncertainties. Just going through the process could be educational for consumers and producers. For instance, as Shell did, being the best prepared in the two oil crises. Scenario methodology changed the decision-makers' mind-sets about the future and its predictability, concept which some analysts are still nowadays behind and discussing about it. The end-goal of scenario building is to be prepared for the future, instead of the obsession of some to predict or guess how the future will look like. Under a scenario approach, estimating is even a bit reckless; scenarios synthetize facts and trends, and reduce the area of the unknowns for the organisation, the analyst or the consumer.

Lastly, the experience of private and public sector engaging into scenario techniques and processes bridges the gap between both [sectors]. The experience with Shell, and later through the US and the UK strategic products, in particular, enrich the field and contribute to strategic analysis and long range estimative intelligence. By shortening the distance, in the case of Scenario Analysis, it is evident that private industry, other disciplines and business planning (in the case of this paper) can contribute positively to the intelligence analysis field, namely through the use of new analysis techniques. On the one hand, scenarios coming from the Oil and Gas industry contributes to intelligence analysis, and on the other hand, SATs could be applied not just for scenarios in the intelligence field, but also to be used in the scenario building process in the private sector as well.

Endnotes:

*01_* *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*. US Government. 2009. Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf

*02_* Heuer, Richards J., Pherson, Randolph J. Structured Analytic Techniques for Intelligence Analysis. 2nd. CQ Press, 2014. 384p.

*03_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.7

*04_* Chermack, Thomas J., Susan A. Lynham, and Wendy E.A. Ruona. "A Review of Scenario Planning Literature." *Futures Research Quarterly*, 2001: 7-31. p.10

*05_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.8

*06_* Ibid p.9

*07_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.11

*08_* Chermack, Thomas J., Susan A. Lynham, and Wendy E.A. Ruona. "A Review of Scenario Planning Literature." *Futures Research Quarterly*, 2001: 7-31. p.17

*09_* Heuer, Richards J., Pherson, Randolph H. *Structured Analytic Techniques for Intelligence Analysis.* Washington D.C.: CQ Press, 2011.

*10_* CIA. *Tradecraft Review.* Langley: Sherman Kent School, 2005. p.37

*11_* Heuer, Richards J., Pherson, Randolph H. *Structured Analytic Techniques for Intelligence Analysis.* Washington D.C.: CQ Press, 2011. p.119

*12_* Gustafson, Kristian. "Strategic Horizons: Futures Forecasting and the British Intelligence Community." *Intelligence and National Security*, 2010: 589-610.

*13_* Ibid, p.590

*14_* Development, Concepts and Doctrine Centre (DCDC). *Global Strategic Trends - Out to 2040.* Ministry of Defence, n.d.

*15_* National Intelligence Council. "Global Trends." *Office of the Director of National Intelligence.* 2013. http: // www.dni.gov / index.php / about / organization / national-intelligence-council-global-trends (accessed 08 17, 2013).

*16_* See the methodology chapter of both DCDC Global Strategic Trends and the NIC Global Trends publications.

*17_* Van der Heijden, Kees. *Scenarios: The Art of the Strategic Conversation.* 2nd. Chichester: Jhon Wiley & Sons, Ltd, 2005. p.107

*18_* Van der Heijden, Kees. Scenarios: The Art of the Strategic Conversation. 2nd. Chichester: Jhon Wiley & Sons, Ltd, 2005. p.107

*19_* CIA. *Tradecraft Review.* Langley: Sherman Kent School, 2005. p.37

*20_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.28

*21_* Chermack, Thomas J., Susan A. Lynham, and Wendy E.A. Ruona. "A Review of Scenario Planning Literature." *Futures Research Quarterly*, 2001: 7-31. p.18

*22_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.59

*23_* Ibid, p.59

*24_* Ibid, p.101

*25_* Wright, George, and George Cairns. *Scenario Thinking.* New York: Palgrave, 2011. p.30

*26_* Van der Heijden, Kees. *Scenarios: The Art of the Strategic Conversation.* 2nd. Chichester: Jhon Wiley & Sons, Ltd, 2005. p.277

*27_* Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.105

*28_* Wack, Pierre. "Scenarios: Unchattered waters ahead." *Harvard Business Review*, no. 85516 (1985): 73-89. p.77

*29_* Ibid.

30_ Van der Heijden, Kees. *Scenarios: The Art of the Strategic Conversation.* 2nd. Chichester: Jhon Wiley & Sons, Ltd, 2005. p.102

31_ Sharpe, Bill, and Kees Van der Heijden. *Scenarios for Sucess.* Chichester: John Wiley & Sons, Ltd, 2007. p.63

32_ Van der Heijden, Kees. *Scenarios: The Art of the Strategic Conversation.* 2nd. Chichester: Jhon Wiley & Sons, Ltd, 2005. p.94

33_ Chermack, Thomas J., Susan A. Lynham, and Wendy E.A. Ruona. "A Review of Scenario Planning Literature." *Futures Research Quarterly*, 2001: 7-31. p.18

34_ Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.139

35_ Ibid, p.140

36_ Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.199

37_ Ibid 192

38_ Pherson, Randolph H., Pyrik, John. *Analyst's Guide to Indicators.* Virginia: Pherson Associates LLC., 2017. P.26

39_ Ibid 192

40_ Chermack, Thomas J., Susan A. Lynham, and Wendy E.A. Ruona. "A Review of Scenario Planning Literature." *Futures Research Quarterly*, 2001: 7-31. p.17

41_ Russell, Richard L. *Sharpening Strategic Intelligence.* Cambridge: Cambridge University Press, 2007. p.49

42_ Berkowitz, Bruce D. "US Estimates of the Soviet Collapse: Reality and Perception." *International Journal of Intelligence and Counterintelligence*, 2008: 237-250.

43_ Russell, Richard L. *Sharpening Strategic Intelligence.* Cambridge: Cambridge University Press, 2007. p.50

44_ Schwartz, Peter. *The Art of the Long View.* 2nd. New York: Crown Business, 1996. p.54

45_ Ibid, p.55

46_ Ibid.

47_ Lowenthal, Mark M. "Towards a Reasonable Standard for Analysis: How Right, How Often on Which Issues?" *Intelligence and National Security* Vol.23, no. No.3 (2008): 303-315 p.313

48_ Betts, Richard K. *Enemies of Intelligence.* New York: Columbia University Press, 2007. p.12

49_ Wright, George, and Paul Goodwin. "Decision making and planning under low levels of predictability: Enhacing the scenario method." *International journal of Forecasting* 25 (2009): 813-825.

50_ Wright, George, and George Cairns. *Scenario Thinking.* New York: Palgrave, 2011. p.16

51_ Chermack, Thomas J. "Improving decision-making with scenario planning." *Futures* 36 (2004): 295-309.

52_ Wright, George, and George Cairns. *Scenario Thinking.* New York: Palgrave, 2011. p.16

53_ Friedman, Jeffrey A., Zeckhauser, Richard. „Assessing Uncertainty in Intelligence." *Intelligence and National Security* 27, no. 6 (2012): 824-847. p.846

54_ Wright, George, and Paul Goodwin. "Decision making and planning under low levels of predictability: Enhacing the scenario method." *International journal of Forecasting* 25 (2009): 813-825.

55_ See Steury, Donald P. *Sherman Kent and the Board of National Estimates.* Washington, D.C.: Booklife, 1994. p.133

56_ Chermack, Thomas J. "Improving decision-making with scenario planning." *Futures* 36 (2004): 295-309.

57_ Klayman, Joshua, and Shoemaker Paul L.J. "Thinking About the Future: A Cognitive Perspective." *Journal of Forecasting*, 1993: 161-168. p.161

58_ Ibid, p.183

59_ Wright, George, and Paul Goodwin. "Decision making and planning under low levels of predictability: Enhacing the scenario method." *International journal of Forecasting* 25 (2009): 813-825.

60_ Ibid.

61_ Chermack, Thomas J. "Improving decision-making with scenario planning." *Futures* 36 (2004): 295-309. p.298

62_ Lowenthal, Mark M. "The Intelligence Time Event Horizon." *International Journal of Intelligence and CounterIntelligence* 22, no. 3 (2009): 369-381. p.369

63_ Kaplan, Oscar. "Prediction in Social Sciences." *Philosophy of Science* 7, no. 4 (1940): 492-498. p.468

Addressing the Internal Challenges to Intelligence Work

Aleksandra Bielska[i]
Chris Pallaris[ii]

Abstract

Intelligence services spend the bulk of their time studying events in their external environment. However, the most pressing problems tend to be found inside the services themselves. Experience has shown that an organization's ability to generate intelligence or communicate warning is proportional to the quality of its processes and workflows. Unfortunately, the design and management of these workflows is rarely given the time and attention it deserves. Consequently, operational challenges are left to multiply. Those charged with addressing them look to do so using toolkits that are worryingly limited. As a result, solutions tend to be ad hoc and poorly designed. This need not be the case. As with intelligence analysis, there are hundreds of techniques one can employ to improve how an organization thinks and works. All that's needed is an open mind and a willingness to exercise one's critical, creative and conceptual thinking skills. This paper discusses the principles of improving organization's processes and workflows, and the tools one might employ to do so. It draws from our experience as consultants to the intelligence community as well as our work on the EU-funded Visual Analytics for sense-making

i i-intelligence GmbH (Switzerland. Email: a.bielska@i-intelligence.eu

ii i-intelligence GmbH (Switzerland. Email: c.pallaris@i-intelligence.eu

in Criminal Intelligence analysis (VALCRI) project (www.valcri.org), and the Global Crisis Response Support Program (www.gcrsp.eu), an extended capacity building project for analysts working in the Americas and the Caribbean.

***Keywords*:** intelligence, intelligence analysis, operations management, process management, workflows management

Introduction

Over the past seven years, we have had the privilege of working on a number of European Union-funded projects aimed at improving the intelligence capabilities of EU member states. During this time, we conducted extensive research into the challenges that analysts and their superiors face. Our research consisted of surveys, interviews and field visits designed to examine the daily realities of analytic work. We reached one inescapable conclusion as part of this effort: while intelligence organizations typically focus on the analysis of external challenges, their efficiency and effectiveness is undermined by challenges that are internal and operational in nature. The character of these challenges suggests a marked deficit in their ability to manage the processes and workflows that form the backbone of an organization's activities. The resulting problems multiply and snowball through an organization, leading to inefficiencies that hamper the organization's ability to adapt or generate value.

While some inefficiency is inevitable in any organization, persistent inefficiency is a problem that demands immediate attention. The article argues that turning analysts into more capable process managers is the remedy to this problem. To do this, it is necessary to extend the analyst's toolkit. Typically, this toolkit is limited to structured methodologies to support intelligence analysis. These methodologies should be supplemented with tools to analyze an organization's policies and processes. Experience suggests that these tools are the simplest way to overcome operational bottlenecks, drive organizational learning, and enable continuous improvement.

To test this hypothesis, we ran a series of workshops that introduce analysts to techniques dedicated to workflow and processes improvement. The workshops were organized under the auspices of the Visual Analytics for sense-making in Criminal Intelligence (VALCRI) project between the Fall 2016 and Spring 2017. Their success provides a compelling case for the development of these capabilities within intelligence teams and larger intelligence organizations.

We detail our research below, starting with a summary of the two most recent

projects we participated in, VALCRI and the Global Crisis Response Support Program (GCRSP).

The VALCRI and GCRSP Projects

VALCRI is a four year, EU-funded project led by Middlesex University. The project is intended to enhance criminal intelligence analysis through a suite of advanced data processing, analytic and sense-making tools. VALCRI acknowledges that technology works best when it augments the cognitive abilities and contextual circumstances of the analyst. The objective therefore is not just to improve the analyst's technical toolkit, but also identify and address varying deficiencies in their non-technical abilities.

The GCRSP was a two-year project dedicated to enhancing the early warning and crisis response capabilities of stakeholders in the Caribbean and Latin America. The project took a holistic approach to capacity development. Tailored programs provided staff at all levels of the organizational hierarchy with instruction in capabilities far beyond the traditional intelligence curriculum (e.g. business process analysis, organization design, etc.). Internal consultancies and project offices were established to further ensure that the skills provided were internalized and strengthened.

Together with earlier initiatives,[1] VALCRI and the GCRSP provided access to analysts working in different functions around the world. We have had a unique opportunity to observe individual analysts and analytic teams at work, conduct interviews, and administer surveys that helped us fill gaps in our understanding of how analysis is done and – most importantly – what are the key challenges to the analytic process. The identified challenges are described below.

The Challenges to Analytic Process

Saying that analysis is a challenging endeavor should not come as a surprise. The tasks associated with it are many, varied and labor intensive. They are often performed in complex organizational settings. "Think[ing] clearly and writ[ing] well", capabilities once praised by Anthony Lake, a former director of policy planning for President Carter,[2] are no longer sufficient to overcoming the challenges to the analytic process. Typically, these challenges emerge as setbacks that stop, slow, or delay progress. *Table 1* below maps these challenges to a typology of inefficiencies from the field of lean management. Doing so provides analytic context and allows us to identify the appropriate solutions and response mechanisms.

Type of Inefficiency	Definition	Observed Challenges to Analytic Process
Motion	Refers to the excessive movement of employees as they are completing necessary tasks, searching for items, etc.	Analysts spend much more time searching for information than analyzing it. It is not unusual for a criminal intelligence analyst to access a dozen different databases to complete a single task. To make matters worse, each database works differently, and different steps and knowledge are needed to use it. Access limitations amplify such headaches. In one organization we surveyed, analysts use a separate workstation to retrieve name plate recognition (NPR) data. The analyst wishing to use this system has to leave her desk to do so. There is only one such workstation available to complete this task so she often has to wait her turn. Another common problem is associated with the need to keep up-to-date with news and social media. Unless an aggregator is available, the analyst has to review multiple websites, intranet pages, and database entries. Accessing each source separately consumes time that could be spent analyzing information.
Transportation	Refers to the excessive movement of information, intermediate or final products, etc.	Analysts lack tools that satisfy their multiple needs. Hence, they spend a considerable amount of time moving pieces of information between databases, Excel spreadsheets, Word documents, and other software applications.

Type of Inefficiency	Definition	Observed Challenges to Analytic Process
Waiting	Refers to waiting for information, equipment, etc.	Analysts depend on other analysts and non-analytic staff. Their work is further influenced by available technology. Accordingly, analysts often have to wait before completing their assignments. For example: · An analyst has to wait on the IT department to address a routine technical issue. · An analyst has to wait for somebody who knows how to use a particular database to help her retrieve relevant data. · An analyst has to wait for collectors to provide her with the information requested. · The software used is slow and/or crashes.
Over-processing	Refers to duplicating tasks, doing more than necessary, etc.	Process and task duplication occur for varying reasons. They can be a consequence of poor knowledge management, information sharing, and collaboration. Duplication occurs as analysts fail to reuse inputs produced earlier, generated in other parts of the organization, or outside of it.
Over-production	Refers to producing items that are not currently needed.	It is not unusual for analysts to write reports no one reads. Intelligence units and organizations often fail to measure and monitor readership. Over-production also occurs when organizations collect redundant information that clutters their systems. Typically, the roots of both problems can be traced to poorly defined requirements.

Type of Inefficiency	Definition	Observed Challenges to Analytic Process
Defects and Complaints	Associated with errors, rework, decision makers' complaints, etc.	The accuracy of analytic products is a priority. Still, these products occasionally contain errors resulting from biased reasoning, use of faulty information, reuse of old data without the necessary updates, superficial analysis, etc. Elsewhere, analytic products routinely fail to meet decision makers' requirements. Our research indicates that many intelligence organizations lack processes to support effective requirements planning. As a result, decision makers complain that what they get is not what they need. Meanwhile, analysts complain that decision makers do not know what they need.
Design	Occurs when one's equipment is not designed to support ease of use, or when the design of premises inhibits productivity, etc.	The software analysts use is often slow, buggy, and overly complex. An analyst has to go through many steps to achieve the intended result. She can rarely proceed quickly using a simple, straightforward process. Moreover, design issues can also impact the premises in which analysts work. For example, analysts complained about their offices being designed to look like an action movie set with dark walls and dimmed lights. However attractive this might seem in a movie, the analysts affected agreed that the design of their office lowered their productivity by making them feel sleepy and enervated.

Type of Inefficiency	Definition	Observed Challenges to Analytic Process
Technology	Refers to a variety of IT issues, including the lack of proper IT training among staff.	Evidence suggest that intelligence organizations continue to invest vast sums of money in IT systems that do not meet their requirements. At the same time, the analysts usually know little about technology. Alas, the less analysts know about their technical tools, the less likely they are to make technology work in their favor (including to press for low-cost or no-cost solutions to routine intelligence problems).
Dataflow	Refers to problems with the flow of data and information.	Poor information sharing between intelligence entities is a well-known problem. This lack of information sharing is a critical issue not only between departments, but also within individual analytic teams. In other words, analysts who sit in adjacent cubicles and belong to the same unit are no more likely to share information than analysts from different departments or organizations.
Performance, Ideas and Talent	Refers to a situation when best practices are not implemented; there is no effort aimed at continuing improvement of performance, the management of talent and the development of staff; decision makers and employees' ideas and suggestions are not captured and acted upon, etc.	By most accounts, the majority of intelligence organizations lack the tools or policies needed to support the continuous improvement. Best practices are rarely and inconsistently implemented, and little is done to develop better practices still. Employees have ideas on how to improve their work. However, there are no mechanisms to encourage them to share these ideas or to enable the implementation of change. To the contrary, many "reformers" must overcome substantial opposition and often give up before the

Type of Inefficiency	Definition	Observed Challenges to Analytic Process
		changes materialize. Feedback from decision makers, even if collected, is also rarely used. Moreover, many organizations struggle when it comes to the management of talent and the development of staff. For example, training programs are rarely subject to careful scrutiny and objective evaluation, which means they are not redesigned even if they bring little or no benefit. Worse still, many intelligence units and organizations suffer from high staff turnover and reluctantly invest in staff members who they expect will soon leave to join another organization or unit. Varying factors contribute to high staff turnover, with the lack of clearly defined opportunities for career advancement and a higher status associated with operating "in the field" being among the most frequently mentioned problems.

Table 1: Examples of challenges to analytic process and corresponding inefficiencies.

The challenges mentioned above prompt the following reflections:

- To begin they are all generic in nature. In other words, they affect both non-intelligence and intelligence organizations. However, until now, solutions have been sought by non-intelligence practitioners. It stands to reason that this is where we should look for guidance.
- They evolve into inefficiencies that are often mischaracterized. For example, poor processes waste resources. While analysts blame resource constraints for their problems, a careful examination of root causes often reveals a different picture. Analysts complain about the lack of time to implement structured analytic techniques. Yet, a lot of

time is wasted searching for information, producing redundant outputs, completing unnecessary tasks, etc.

- Automation does not produce the right results; the right processes do. Consequently, automation is not enough to boost efficiency. Automating bad processes is a problem, not a solution.
- The poor handling of information causes many of the inefficiencies listed above. Although information is our main tool of work, analysts often lack a basic grounding in disciplines such as information governance and information management. As a result, they lack the ability to handle information in a way that conserves time and effort while also supporting analysis.

A lack of awareness is not why these challenges persist. Analysts and their managers are aware of these problems. In fact, they are the ones who typically signal a need for change. They are also willing to invest their time and effort to develop and implement the necessary solutions. The problem is that they are not given the right tools or knowledge to do so. Our experience as trainers and consultants to intelligence services has taught us that what these professionals need is a basic understanding of disciplines such as operations management, process analysis, and workflow improvement. The next section summarizes what these disciplines are and how they can be of value to intelligence organizations.

Improving Operations, Processes, and Workflows

As Anderson, et al. explain, operations management is "the science of managing resources and behavior".[3] It ensures that the people, policies, processes, and resources associated with routine or ad-hoc activities are managed in a way that enables the most efficient realization of an organization's goals. Related practices allow organizations to optimize resource allocation while also improving the quality of their outputs and processes. Further, they orient staff around clear outcomes and a consistent understanding of internal (e.g. staff training and development) and external (e.g. customers' needs and expectations) pressures on the organization's operations. Operations management is an umbrella term which encompasses process and workflow management, together with additional disciplines, such as general management, change management, project management, etc.

Quoting Amatayakul, a process is "the manner in which work is performed".[4] Organizations develop processes that reflect their unique context. Process management enables the efficient execution of processes and allows organizations to meet their goals despite changing conditions. It also helps them address the variability and complexity commonly associated with process implementation.

Process management includes efforts aimed at:

- Setting and monitoring goals that provide clear and uniform direction, facilitate planning and prioritization, enable monitoring and the evaluation of progress, and foster understanding between team members;
- Documenting and standardizing processes that help reduce complexity and achieve consistency throughout the organization. This facilitates the induction and training of new team members. Documentation and standardization also help to eliminate redundant or unnecessary procedures and, hence, increase the efficiency of tasks;
- Evaluating and improving processes and products, which enable the minimization of cost and waste while maximizing value-added. Doing so improves the quality of outputs and increases productivity, while also contributing to increased satisfaction and morale among employees;
- Identifying, understanding and fixing bottlenecks and other inefficiencies. This includes a careful analysis of root causes and possible remedies. The processes can be streamlined and resources saved as problems are discovered early and resolved quickly and precisely;
- Effective management of interactions between processes, including optimization of the way in which processes share similar resources;
- Simplifying processes to make them easier to understand, manage, and monitor;
- Streamlining processes by use of technology and after careful consideration of what to automate and how;
- Effective management of associated information and knowledge flows. This ensures that the right information reaches the right people, at the right time;
- Optimizing resource allocation, leading to the effective use of time, money, people, space, and other resources;
- Effective allocation of responsibilities to ensures the efficient use of talent, time, and money. If properly executed, this also increases job satisfaction and motivation among team members.

There is no generally accepted definition of "workflow".[5] Occasionally, this term is used interchangeably with the "process".[6] For the purpose of this paper, however, we distinguish between workflows and processes applying a definition proposed by Amatayakul. Accordingly, we define a workflow as "the sequence of steps or hand-offs within a process and between processes".[7] To understand the difference between processes and workflows, consider an analyst who uses a structured methodology to evaluate a source. The steps the analyst takes form a workflow. They represent a distinct sequence of activities that are repeated in

relation to each source and can be easily distinguished as related to the same intermediate goal. The whole sequence is part of a larger process aimed at the analysis of the data collected.

Workflow management is all about managing the flow of work in a way that ensures it is tuned for maximum efficiency. Similar to process management, workflow management allows organizations to identify and minimize waste. Workflow management also consists of corresponding stages which include: definition and modelling, analysis, redesigning, implementation, and continuous improvement. The redesign of workflows can involve the elimination of unnecessary tasks, the addition of controls to monitor performance, dividing and combining tasks, etc.[8] Traditionally, workflows are also optimized through automation. As a result, many researchers use the term "workflow" to describe any process or sub-process that can be automated.[9] Process and workflow management work best when applied together as recurrent practices. The deficiencies they address cannot be cured overnight. Rather, remedies have to be implemented as part of a gradual, systematic, and continuous effort.

Operations, Process, and Workflow Management in Intelligence

Exposing analysts to process and workflow management is ultimately the best test of the value of these disciplines to intelligence analysis. This was done during the series of workshops organized under the auspices of the VALCRI project. Each workshop lasted three days. Day 1 demonstrated how to define and evaluate existing workflows and processes. Day 2 introduced the concept of design thinking to help analysts develop new processes and improve cross-functional collaboration. Day 3 invited participants to use previous outputs to determine where and how to embed structured analytic techniques into their current activities.

The feedback generated was overwhelmingly positive. The analysts stated that the workshops gave them the ability to improve how they plan and organize their work. They also felt that having a richer problem-solving toolkit would allow them to add more value to their teams. They explained that the tools provided would let them address organizational challenges without waiting on senior management to do so. As one analyst observed, if there is a problem, there is always a tool that can be used to solve it. This is particularly interesting as it suggests the workshops empowered participants to become active shapers of their operating environment. That a workforce is engaged and confident is a positive side-effect. Borrowing from Stanford, "The more everyone in an organization feels in some control of what is going on, and has input into it, the more likely it is that the end result will be one that they are motivated to work in; that is, they will be committed rather than simply compliant".[10]

An Extended Analytic Toolkit

There are hundreds of techniques one can employ to improve how an organization thinks and works. These tools aid decision making and action taking by strengthening critical, creative, and conceptual thinking. The tools used to support operations, process, and workflow management represent a small but still sizable subset of all the tools available. They allow analysts to: (1) analyze processes and workflows from all possible dimensions, (2) critically evaluate assumptions and conclusions, (3) generate ideas and identify unorthodox ways to carry out tasks and solve problems, (4) explore and understand patterns and relationships, and (5) effectively organize ideas for greater clarity. These tools can be divided into four categories:

- *Definition and Mapping,* which includes tools that help to identify key processes and workflows and understand how they proceed. Tools in this category include, for example: Process and Workflow Inventories, Process and Workflow Maps, Process and Workflow Flowcharts, Gantt Charts, Surveys, Interviews, Focus Groups, etc.
- *Analysis and Redesign,* which includes tools that enable in-depth understanding of processes and workflows, help to identify and examine related problems, and assist in process reengineering. Tools in this category include, for example: the POLDAT Model, Root Cause Analysis, Issue Trees, Pareto Analysis, ICOR (Inputs, Outputs, Controls, Resources) Analysis, Start – Stop – Continue, Business Process Redesign (BPR), etc.
- *Implementation,* which includes tools that enable smooth implementation of reengineered processes. Tools in this category include, for example: SMART Goals, Force Field Analysis, the RACI Matrix, Stakeholder Analysis, Checklists, etc.
- *Continuous Improvement,* which includes tools used to ensure that workflows and processes are subject to continuing evaluation and enhancement. Tools in this category include, for example: PDCA / PDSA, OODA, Catchball Process, Kaizen, Gemba, Bottleneck Analysis, etc.

Optimally, the analyst should also be familiar with the principles and tools associated with such disciplines as:

- *Change Management,* which ensures that changes are effectively implemented.
- *Project Management,* which - for good reasons - is often considered a risk area in relation to operations, process, and workflow management.[11] It ensures that any initiative is properly planned and implemented.

- *Leadership,* as good leaders are needed to sustain high morale, motivation, and productivity in times of change and beyond; nurture people and ideas; and ensure that organizational culture remains flexible and open to change.
- *Information Governance and information Management,* which ensure that the information flows accompanying processes and workflows are efficiently and securely managed.
- *Individual and Organizational Learning,* which ensure a constant supply of new skills and knowledge that are key to sustained performance improvement.

Put simply, the more tools the analyst has – and knows how to use – the better. These tools can be used to explore the different facets of a problem, and to surface different perspectives. They can also be combined to construct novel solution pathways, or to fully explore the complexity of a specific issue. More pressingly, these tools teach analysts how to think, specifically, how to engage in different modes of thinking (critical, creative, lateral, sequential, holistic, etc.). The richer their toolkit, the richer their thinking is likely to be, and the better the analytic products that they go on to produce.

Conclusions

The challenges analysts face in the workplace are considerable. Process, and workflow management are not the only disciplines needed to improve an organization's analytic outputs. Leadership, change management, and information governance are other areas worthy of greater attention. Indeed, there are many disciplines of potential value that receive little attention from those who study or work in intelligence. It is essential that we bridge these gaps in our knowledge. Absent the right tools, resources are wasted, failures multiply and, in extreme cases, lives are lost. The VALCRI and GCRSP projects have shown how much can be achieved by extending the analyst's skills beyond those common to the intelligence cycle.

Going forward, our objective is to explore disciplines additional to the ones covered during these projects. We also plan to synthesize and turn all findings gathered as a result of our past and future research into formal recommendations on the training and development of intelligence professionals.

Endnotes:

*01_* Including the EU-funded RECOBIA project and few smaller engagements.

*02_* Anthony Lake, *Somoza Falling* (Boston: Houghton Mifflin Company, 1989), 215.

*03_* Mary Ann Anderson, et al., *Operations Management for Dummies* (Hoboken, NJ: John Wiley & Sons, Inc., 2013), 28.

*04_* Margret Amatayakul, *Electronic Health Records: A Stepwise Approach to Workflow and Process Management* (Boca Raton, FL: CRC Press, 2012), 19.

*05_* Hajo A. Reijers, *Design and Control of Workflow Processes: Business Process Management for the Service Industry* (Berlin, Germany: Springer, 2003), 20.

*06_* Wil M.P. van der Aalst and Kees van Hee, *Workflow Management: Models, Methods, and Systems* (Cambridge, MA: The MIT Press, 2002), xvi.

*07_* Margret Amatayakul, *Electronic Health Records: A Stepwise Approach to Workflow and Process Management*, 20.

*08_* For more information, please see: Hajo A. Reijers, *Design and Control of Workflow Processes: Business Process Management for the Service Industry*, 207-242.

*09_* Asuman Dogaç, *Workflow Management Systems and Interoperability* (Berlin, Germany: Springer, 1998), 357; Hajo A. Reijers, *Design and Control of Workflow Processes: Business Process Management for the Service Industry*, 18.

*10_* Naomi Stanford, *Guide to Organisation Design* (London, UK: Profile Books Ltd., 2015), 35.

*11_* Hajo A. Reijers, *Design and Control of Workflow Processes: Business Process Management for the Service Industry*, 16.

The Practice of Intelligence in Emerging Economies: the Exploratory Case Study of Peru

Juan Carlos Ladines Azalia[i]
William Castillo Stein[ii]

Abstract

The function of intelligence has changed in recent decades. In a globalized world, the incorporation of new threat or opportunity variables into intelligence analysis has modified its practice. Currently, the literature calls for an opening of the field, and due to this, intelligence research has evidently grown. Nevertheless, the existing literature is at best incomplete, since its main focus is on Anglo-Saxon and Western European countries. There has not been a literature on intelligence in emerging economies. In this article, we conduct an exploratory research case study on intelligence in Peru, with the aim of discovering insights into this matter. In addition, it is also an opportunity to invite other scholars to engage in further research on this topic.

This exploratory research retrieves valuable insights into intelligence in Peru based on in-depth semi-structured interviews with three scholars with past experience, working with the private or governmental sector. The result showed the existence of an evident gap between academia on the one hand, and the

i Universidad del Pacífico, Peru. Email: ladines_jc@up.edu.pe.

ii Universidad del Pacífico. Email: w.castillostein@alum.up.edu.pe.

corporate world and Government on the other, mainly because of the secrecy culture. On more open issues, however, academia works well with the other sectors, mainly providing expert opinion and counseling. At the same time, as shown in this article, at an intermediary degree, there is also communication space between the three fields through informal channels.

***Keywords*:** Intelligence, Peru, emerging economies, information management, moral hazard.

Historically, intelligence has been used by political structures in order to ensure power configurations. However, it only began to develop as a field during the 1950s, especially as a result of the founding work conducted by Sherman Kent[1]. In the years to follow, but especially during the past decade, the literature on intelligence has developed considerably, taking the form of a multidisciplinary field of study[2]. Nowadays, in a globalized world, the subject of intelligence has exceeded topics circumscribed to military affairs, and has incorporated new sectors and practices, such as cybersecurity, (counter-) terrorism, and financial security[3]. Nevertheless, while these observations apply to the literature on intelligence in the United States, Canada, United Kingdom and a few other Western European countries, where the scholarship continued to expand[4][5], there is not a similar trend in emerging economies.

To talk about emerging economies means to reconsider the conventional North-South divide. Emerging economies can be described as countries undergoing fast-paced turbulent change as a result of economic liberalization, rapid industrialization and increased interaction with the global arena[6]. In these types of economies, while economic progress has become stable, they are still institutionally weak. Nederveen Pieterse[7] describes emerging economies as "[countries with] rising levels of development and gradually rising influence in the vicissitudes of globalization" (p. 3). Overall, they present a different context than in developed countries, which is worth studying from the perspective of its potential impact on the practice of intelligence.

While emerging economies are heterogeneous among themselves, a focus on the top twenty emerging markets[8] would add most value to the practice of intelligence in different contexts, since these are the countries gradually gaining more influence in the global arena. Thus, while still lacking hard power in the global arena[9], emerging economies can exercise their soft power, as global players, actors, or stakeholders, which requires intelligence to adapt its support to decision-makers and the policymaking process accordingly. As an exercise, disseminating information by intelligence agencies, or other relevant institutions, will serve the purpose of persuasion in world politics[10]. Moreover,

paying more attention to the security culture and intelligence communities developing in these types of economies provides a perspective beyond the traditional Anglo-Saxon/Western approach, with the findings even having the potential to challenge conventional thought. For the academic community, it nourishes the theoretical debate of intelligence, as an ongoing discussion. For practitioners, it helps them understand the practice of intelligence under different institutional contexts, which reduces risk in strategy formulation and decision-making for foreign policy.

In the developed world with a strong institutional context, the practice of intelligence can be done with higher "certainty," whereas in low institutional context situations, the intelligence products and future scenarios produced cannot be given this certainty. As showed by Ladines & Castillo[11] who analyzed state planning institutions within the Pacific Alliance (Chile, Colombia, Mexico and Peru), there is a lack of a forward-looking, prospective planning, which is translated into a lack of knowledge as to what kind of information is relevant for intelligence analysis and decision-making. Thus, it is in these types of suboptimal cases that academia is most needed to support practitioners' decisions and policies.

According to Stephen Marrin[12], the development of a field of intelligence requires academics to engage in: (1) documenting what is known, (2) evaluating it for gaps; (3) working to fill the gaps in knowledge; (4) distributing the knowledge; and (5) institutionalizing it. To Marrin's observation, this article adds two other necessary engagements of the academic environment. On the one hand, scholars should extend their geographical area of research to include less studied communities of practice; on the other hand, the members of the academic environment, especially security and intelligence scholars from countries less represented in the literature should be more actively involved; they should assume and enforce new practices, as well as disseminating new knowledge beyond their institutional or national academic communities.

Since different contexts serve to test existing theories or develop a new theory,[13]- and given the proliferation of emerging economies in the past decades[14], it becomes relevant to develop a literature that includes the study of intelligence in these countries. With this in mind, the present article aims to contribute to the intelligence literature, offering an emerging economy perspective on intelligence issues through a working exploratory research of the Peruvian case. Moreover, this article seeks to encourage other scholars to engage in further research on intelligence from these regions.

For the purpose of conducting an exploratory research, this paper used in-depth semi-structured interviews of three scholars. As a filter, it was necessary they had past experience working with the corporate and governmental sectors on intelligence issues. Their respective background was accounting, economics, and ethics. Through the use of literature and interviews, a case study of

Peru was developed, following Robert Yin's[15] case study methodology[iii]. As Eleanor Shaw[16] argues, the case study methodology permits discovery, interpretation and comprehension, and therefore reflects a perspective of a socially constructed reality. The interviews were structured in four sections. To begin with, the scholars were asked to talk about their past experience and describe the role that academia had in the dissemination of intelligence among the public and private sector. Secondly, they were questioned about the role of academia in Peru, in relation to the other sectors, as well as the benefits or downfalls of a closer relation. Thirdly, they were asked about the practice of intelligence in Peru, and to comment if there has been a change following the Neoliberal reforms of the 90s, which most emerging economies applied. Finally, based on their past experiences, they were asked to describe the future of the relationship between academia and the private or public sector in Peru.

The most important insight drawn from the interviews was that due to different social norms between academia and the private-public sector, intelligence from the academic sector is *separated* from intelligence in the corporate or public sector. In other words, the findings contrast with the existing literature, which advocates for a closer relationship between the three worlds for the purpose of knowledge building. In the case of Peru, this process has not been assumed yet. This article does not aim at providing a definitive conclusion; further research in the case of other emergent economies is still required, however, this research aims at giving an incentive on the importance of studying intelligence under different (national) contexts. Such an endeavor has the merit to test the argument hitherto advanced in the literature about the value of developing a cross-sector dialogue among Intelligence stakeholders in countries with different security, economic and political cultures than Western Democracies.

Thus, in this context, intelligence stakeholders are faced with different security and political culture. For example, the practice of intelligence must take into account the interplay between regional and global levels of security, since this largely shapes the operational and political environment[17]. Moreover, Mohameed Ayoob states that the definition of security should be primarily political[18], given their vulnerability in this realm. Even more, cultural identities from non-Western societies are shaping the regional or global patterns of cohesion, disintegration and conflict[19].

Peru, just as other emerging economies, is undergoing turbulent changes on various dimensions, such as social, political, economic and technological

iii According to Robert Yin, a case study research is preferred when answering open-ended questions, such as "how" or "why" questions. In these types of research, there is little control over events, and it is focused in a real-life context. All these prerequisites are fulfilled by this research.

that are integrated in the security culture and have become relevant for the IC's activity. For example, the BRIC (Brazil, Russia, India, and China) economies have been characterized for turbulent economic growth[20]. Similarly, emerging economies from transitional economies of the former Soviet Republic have had political turbulence[21]. In the same manner, emerging economies face social turbulence, given the disparities between rural and urban areas, as well as the struggle with urban poverty[22]. Consequently, these changes require a more inclusive definition of intelligence able to express the emergence of new security stakeholders and the 21st century challenges that the world knows. Thus, among the numerous definitions of intelligence that has been advanced by different scholars, Breakspear's[23] has pushed the threshold of the concept into new dimensions otherwise overlooked. The author defines intelligence as:

> "(…) a corporate capability to forecast change in time to do something about it. The capability (…) is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat" (p. 688)

This definition views intelligence as a corporate capability, which means that private and academic entities qualify as both intelligence producers and consumers, becoming active players of the intelligence community (IC).

Furthermore, the literature highlights that the incorporation of new variables and stakeholders into intelligence analysis have generated the need to integrate the academic sector into the intelligence community. Indeed, both intelligence practitioners and scholars have had to deal with the expanding notion of threats, and the need to develop a joint research agenda with the aim of understanding, explaining and improving intelligence analysis[24]. As Gearson[25] states: "Operational concerns of education, security, and intelligence meet academically at the interface of education, security, and intelligence studies" (p. 275). Thus, the author notices that an overlap could occur between the intelligence practitioners and scholars, creating a mutually beneficial relationship and a knowledge building process. This matter is also emphasized by Stephen Marrin[26], who emphasizes that: "The contribution that higher education makes to interpreting its past, understanding its present, and forecasting its future. It forms a body of knowledge that is academic (…) yet useful for the intelligence professional (p. 266). The American scholar takes into consideration a possible overlap between the intelligence practitioners and academics, and affirms the formation of a body of knowledge, useful for both.

Although the literature encourages a better relationship between the three worlds, in Peru, nevertheless, this gap is not being bridged. There is a deficient relationship between the academic sector, private sector and public sector as it

was emphasized in three interviews conducted with academic scholars[iv] about the practice of intelligence in Peru.

First, according to the interviews' findings, the intelligence discourse is not formally developed in the academic sector. Rather, it is considered as an elephant in the room, and is mainly a "gossip". For the Peruvian case, given a weak context[v] of the country, talking about such delicate matters could translate into negative connotations. In the interviews, the scholars stated that intelligence is a central focus in academia, thus it lacks theoretical foundations. It is referred to with negative connotations because of a lack of definition in the cross-sector dialogue, so most actors assume that intelligence is used in a zero-sum nature. In effect, since it was an informal matter, there was not a clear definition of what intelligence is or what its functions are.

Second, the academia's relation to the public and private sector, based on practical experiences, can be summarized in the following figure:

Figure 1: The academy's relation to the public or private sector

The figure highlights the practical examples that the interviews gave regarding past interactions between academia and the corporate or governmental world. Even though they perceived a separation between the worlds in the case of Peru, there have been situations when they have come together. These issues can be put on a timeline, depending on the degree of secrecy for the intelligence function. With low levels of secrecy, competitive intelligence has been done, while with high levels of secrecy more informal channels are used.

Third, as previously stated, there have been past experiences where these sectors have come together. In Peru, albeit a gap between academia and the corporate and governmental worlds, the interviews revealed that there have been intelligence issues that have made these sectors come together. According to Gonzalez Vigil[27], collective processes of capacity building based on a dialogue among the

iv As explained in the methodology, the three academic scholars have had past experience working with the corporate and governmental sectors on intelligence issues, which makes them ideal to discuss the practice of intelligence in Peru.

v We follow the definition of institutional context after DiMaggio & Powell that refer to them as way in which schemas, rules, norms and routines become guidelines for social behavior.

three sectors (academia-government-private sector) have been conducted, with each sector contributing to address a specific function. Academia has the tools to provide competitive intelligence[28] and expert opinion. In practice, it has used its capabilities for participating in the negotiation of the Free-Trade Agreement (FTA) between the Peruvian government and the United States of America. In this case, the advantage provided by scholars is that given the low level of secrecy that their work is subject to, they were able to engage and coordinate with a big number of relevant actors. Thus, the production of intelligence by scholars for intelligence consumers (both public and private) was an optimal configuration. Competitive intelligence was provided in the FTA negotiation, because academia understood future needs and changes in the market of their client (public and private). Through expert opinion, they provided intelligence for seeking opportunities and minimizing threats, thereby, negotiating certain issues optimally. Moreover, academia offered technical advice and training on international commerce and negotiation skills, as well as provided methodological and analytical models for a better design and implementation of state policies.

Following Gearson's statements, the interface of education met operational matters, when negotiating the FTAs. González Vigil[29] even mentioned that there was a learning process supported by academia, where the FTAs negotiators took into consideration past errors from the Neoliberal decade of the 90s, and transitioned into a negotiation that considered economic security needs of the Peruvian Trade Unions. Therefore, the actionable intelligence that scholars were able to provide decision-makers with shows that academia's input can turn into descriptive and evaluative analysis products.

A fourth finding based on the interviews has been that on an intermediary degree, the academic sector develops various social events such as forums, congresses, and expert talks, where business people, scholars, and generally government officials get together and exchange information. Although the aim of these gatherings is the dissemination of findings or insights, they also facilitate interactions between decision-makers. Informally and tactically, information is spread out through word of mouth, and although the way in which information is later used is not within the hands of academia, its role in these types of situations has the potential to make a difference by simply channeling spaces of and for strategic communication. Thus, under these scenarios, to talk about a triangular configuration would be incorrect, since academia only provides the means, which intelligence consumers (private and governmental) could use for numerous ends.

In emerging economies with a weak institutional context, intelligence analysis cannot be done with an expected outcome. At the same time, there is not a proper accountability of information and sources, to the point that any "gossip" developed about an issue is valid. Given these contextual factors, the academic community does not engage, nor does it propose methods for the opening of

the practice of intelligence. For top secrecy issues, informal channels are most used, so that a triangular configuration does not take place. These matters have not been dealt with in academia so far, and are considered a main factor for the existence of an intelligence gap.

Now, even though there were practical situations where academia and the private and/or governmental sector have met, the three academic scholars interviewed still stated that from their experience, there is an evident gap and lack of relationship between the sectors (scholars and practitioners), and the blame is shared by both sides. Academically, since an intelligence discourse is not developed, intelligence practitioners are being mentally shaped with a knowledge gap on specific matters of intelligence.

In conclusion, the present paper has caveated the Intelligence discursive gap between academia and the corporate and governmental spheres in countries with emerging economies by considering the case of Peru as representative. Thus, given the absence of an optimal triangular configuration and of a solid cross-sector relationship, bridging the gap becomes important to provide actionable intelligence, and develop accountability in the practice of the IC.

As an emergent economy, Peru shows an evident gap between academia and intelligence practitioners, yet, several past experiences showed that research theory and practice can meet and work efficiently towards a common goal. From the analysis done, intelligence provided by academia is most useful in the case of competitive intelligence, where scholars and subject matter experts (SMEs) can provide expert opinion to both the corporate and governmental sphere. These types of situations tend to become more frequent and able to provide great benefits, such as in the FTA negotiations between Peru and the US. The value from this is that information was disseminated among the three sectors, producing a dialogue. Thus, the public and private sector presented their economic security needs, and academia provided expert opinion and analysis, as well as training on negotiation skills. Information-sharing and knowledge-building, supported by dialogue, produced better results. However, as the interviews concluded, as scenarios shift into more informal or turbulent channels, academia does not become involved in these matters, thus the three sectors *separate*. Academia ceases to provide information and support to decision-making under this informal scenario.

The lack of past institutional experience in developing bridges for dialogue across stakeholder sectors, has hindered the development of reflection on Intelligence within the national context. In theoretical terms, intelligence in emerging economies needs further development for its professionalization. However, a change of mind is necessary in a more applied approach of the practice of intelligence in emerging economies given the current relative power shifts in the global sphere, where countries like Peru are starting to *emerge* as security key stakeholders in political and economic terms. Thus, an expansion of the

literature in emerging economies would serve the purpose of understanding the function of intelligence in different institutional and social contexts, and contribute to future policy and decision-making.

Endnotes:

*01_* Sherman, Kent. Strategic intelligence for American world policy. Princeton, New Jersey, 1949.

*02_* Richards, Julian. "Intelligence Studies, Academia and Professionalization." The International Journal of Intelligence, Security, and Public Affairs 18.1 (2016): 20-33.

*03_* Buzan, Barry, Ole Wæver, and Jaap De Wilde. Security: a new framework for analysis. Lynne Rienner Publishers, 1998.

*04_* Kahn, David. "Intelligence studies on the continent." Intelligence and National Security 23.2 (2008): 249-275.

*05_* Gill, Peter, and Mark Phythian. "What Is Intelligence Studies?." The International Journal of Intelligence, Security, and Public Affairs 18.1 (2016): 5-19.

*06_* Marquis, Chris, and Mia Raynard. "Institutional strategies in emerging markets." Academy of Management Annals 9.1 (2015): 291-335.

*07_* Pieterse, JP Nederveen, and Boike Rehbein. *Introduction: Development and Inequality*. Palgrave Macmillan, 2009.

*08_* Bloomberg. The Top 20 Emerging Markets. Retrieved November 28, 2017, from https://www.bloomberg.com/news/photo-essays/2013-01-31/the-top-20-emerging-markets (2013)

*09_* Nye Jr, Joseph S. "Get smart: Combining hard and soft power." *Foreign Affairs* (2009): 160-163.

*10_* Keohane, Robert O., and Joseph S. Nye Jr. "Power and interdependence in the information age." *Foreign affairs* (1998): 81-94.

*11_* Ladines, Juan Carlos & Castillo, William. "Strategic Planning and Scenario Planning in Public Institutions: The Case Study of Pacific Alliance" FIIB Business Review, Volume 6 Issue 3, 2016.

*12_* Marrin, Stephen. "Improving intelligence studies as an academic discipline." Intelligence and national security 31.2 (2016): 266-279.

*13_* Peng, M. W. (2005). Perspectives - from China strategy to global strategy. Asia Pacific Journal of Management, 22(2), 123-141.

*14_* Wright, Mike, et al. "Strategy research in emerging economies: Challenging the conventional wisdom." *Journal of management studies* 42.1 (2005): 1-33.

*15_* Yin, Robert K. Case study research: Design and methods. Sage publications, 2013.

*16_* Shaw, Eleanor. "A guide to the qualitative research process: evidence from a small firm study." Qualitative Market Research: An International Journal 2.2 (1999): 59-70.

*17_* Buzan, Barry, and Ole Waever. *Regions and powers: the structure of international security*. Vol. 91. Cambridge University Press, 2003.

*18_* Ayoob, Mohammed. *The Third World Security Predicament: State Making, Regional Conflict, and the International System*. Boulder: Lynne Riener, 1995

*19_* Huntington, Samuel P. *The clash of civilizations and the remaking of world order*. Penguin Books India, 1997.

*20_* Wilson, Dominic, and Roopa Purushothaman. *Dreaming with BRICs: The path to*

2050. Vol. 99. New York, NY: Goldman, Sachs & Company, 2003.

*21_* Makhmadshoev, Dilshod, Kevin Ibeh, and Mike Crone. "Institutional influences on SME exporters under divergent transition paths: Comparative insights from Tajikistan and Kyrgyzstan." *International Business Review* 24.6 (2015): 1025-1038.

*22_* Pieterse, JP Nederveen, and Boike Rehbein. *Introduction: Development and Inequality.* Palgrave Macmillan, 2009

*23_* Breakspear, Alan. "A new definition of intelligence." *Intelligence and National Security* 28.5 (2013): 678-693.

*24_* Marrin, Stephen. *Improving intelligence analysis: Bridging the gap between scholarship and practice*. Routledge, 2012.

*25_* Gearon, Liam Education, Security and Intelligence Studies, British Journal of Educational Studies, 63:3 (2015), 263-279

*26_* Marrin, Stephen. "Improving intelligence studies as an academic discipline." Intelligence and national security 31.2 (2016): 266-279.

*27_* González-Vigil, Fernando, Álvaro Henzler Vernal, and Carlos Rueda Heredia. Tópicos de negociaciones comerciales internacionales: metodologías y aplicaciones relevantes para el Perú. Vol. 1. Departamento de Economía, Universidad del Pacífico, 2006.

*28_* Kahn, David. "An historical theory of intelligence." Intelligence and National Security 16.3 (2001): 79-92.

*29_* González-Vigil, Fernando, Álvaro Henzler Vernal, and Carlos Rueda Heredia. Tópicos de negociaciones comerciales internacionales: metodologías y aplicaciones relevantes para el Perú. Vol. 1. Departamento de Economía, Universidad del Pacífico, 2006.

The history of Intelligence: Future Prospects

[i]Constant (C.W.) HIJZEN

Abstract

Recently, several flaws in the intelligence studies have been designated. It lacks a proper body of knowledge, it lacks theories, and it fails to be 'cumulative'. In order to become more academic, intelligence studies should therefore build 'more theories', it is often heard. In this article, it is argued that in addition to this social scientific answer, historians should come up with their own solutions. They can contribute to a body of knowledge and interact with the historiography; however, for this purpose, they have to transcend the particular details of their findings, and interpret their results in the light of a set of core questions or themes, in order to let other benefit from their work.

***Keywords*:** intelligence historiography; study of intelligence; missing dimension; historians; key debates.

Introduction

Intelligence historians and intelligence analysts generally agree that history plays an important role in their work. Establishing more precisely what role intelligence history could and should play in the academic discipline of the intelligence studies, as well as in the practice of intelligence analysis, has been scrutinized less often, however. In this article, it will be argued that – in order to increase the value of historical research for the study and practice of intelligence – historians will need to strive to relate their work to more general themes within the intelligence field.

i Research group Intelligence and Security (Institute of Security and Global Affairs) and the Institute for History at Leiden University (the Netherlands).
Email: c.w.hijzen@fgga.leidenuniv.nl and c.w.hijzen@hum.leidenuniv.nl.

The main point that will be made is that historians will need to analyze their research in the light of broader questions, instead of predominantly in terms of their particular cases; this also involves the implications for intelligence analysis that will be touched upon at the end of the article.

The following example from Dutch intelligence history shows that even a particular event raises questions that relate to themes and topics discussed more broadly within the intelligence studies. On 22 November 1918, Han Fabius, the head of the military intelligence section of the Dutch General Staff, wrote a letter to several police chiefs and a few commanders of the military police. He proposed to establish a civil security service, which was meant to become active after martial law had been replaced with the civilian administration in peacetime again. Because the end of the Great War caused civil unrest and toppling governments everywhere, Fabius and other elements of the Dutch establishment feared that the 'revolutionary steamroller' would inevitably push on westward – for what reason, after all, would revolution stop at the Dutch border, if Russia, Albania, and Germany had already fallen prey to it[1].

Fabius argued, therefore, that a security service should be established under the General Staff of the Dutch army (for the very pragmatic reason that during the First World War intelligence and security activities had been developed there) and he asked the police commissioners, who were to become the primary intelligence producers for the security service, for their opinion. Unexpectedly, they were not very enthusiastic about the idea. Fabius was entering a 'perilous domain', they anticipated.[2]

Karel Henri Broekhoff, an Amsterdam police inspector with whom Fabius had worked closely when in November 1918 revolution appeared to be coming to the Netherlands, was Fabius' most pronounced critic. If the security-service-to-be was to fight the revolutionary threat, a threat that manifested itself out in the *open* - after all, revolutionaries held public meetings, their candidates were publicly known, and their propaganda was widely distributed - then establishing a *secret* service was not an answer to the problem, Broekhoff argued. Secondly, he objected, if Fabius would pursue this anyway, the number of people that had to be involved would soon be so large, that it would be impossible to keep the security service's existence a secret. Broekhoff himself now had some experience in collecting political intelligence in Amsterdam, and he had worked with a very large number of workers, journalists, and police officers. It would hence become public knowledge that the state was spying on its own citizens. This, finally, would have a counterproductive result, Broekhoff wrote Fabius: if society would learn that the state was meddling, mixing, and interfering in the lives of innocent citizens, who were not suspected of committing a crime, then radical socialists (and more broadly, the extremist fringes of the workers' movement) would undoubtedly make use of it for their propaganda, Broekhoff argued. Their narrative would be that the state, already under pressure since November

1918, was illegitimately harassing the workers. Support for and membership of revolutionary organizations would increase, which would be exactly opposite to Fabius' fundamental idea behind this security service: safeguarding the democratic order against the revolutionary threat.[3]

This correspondence about the rationale of establishing a secret service relates to a recurrent and still topical question in the domain of intelligence and security: why, and how, are intelligence organizations institutionalized and embedded? What are their core functions, what do they do in practice and why do they do that? Who tasks and manages them, who reads their reports, how to oversee whether they do not operate outside the law? What are the dominant threats and enemies these organizations have to counter and how exactly should they do that?

These political, administrative, and managerial questions can be asked by practitioners in order to improve the functioning of the intelligence instrument within the state. But these questions can be asked by historians as well in order to improve our knowledge about the function and practice of intelligence and security services. Historical research on intelligence and security services is of crucial importance with the purpose to understand their contribution to policy and decisions in the present, but especially how they have done so in the past, as Richard Aldrich argues. Historical research helps us to understand how during the Cold War policies were underpinned and legitimated by intelligence, and how 'at the lower levels it was the secret services that formed the front line'. As the same Aldrich emphasizes: 'The Cold War was fought, above all, by the intelligence services'.[4] Even though the Cold War has been influential for the way intelligence and security services around the globe have institutionalized and developed over time, their institutional forms, working practices, organizational models, and divergent positions within the broader democratic state can be markedly different. Even the intelligence communities of the United States and the United Kingdom, which are very akin because of their historical ties, differ in important respects. In the United States, there are currently sixteen separate formal intelligence and security services, in the United Kingdom there are three; consequently – and due to differences in political culture and different histories – the American intelligence community is characterized by 'institutional divisions and rivalries', whilst in the British context 'collegiality' is 'endemic'.[5] As a result, Philip Davies concludes that intelligence 'does not mean the same thing on opposite sides of the Atlantic'.[6] What in both practices is meant when the word 'intelligence' is uttered, differs in terms of practices, reports, processes, and organizations. The 'many different ideas of intelligence', therefore, have 'institutional and operational consequences' that we as historians need to understand.[7]

In order to address these national differences in intelligence institutions and practices, including in intelligence analysis, historians could try to analyze them from a comparative perspective. In the historiography on intelligence and

security services, however, such an approach has not been chosen very often.[8] Generally, historians tend to present stand-alone cases and stick to telling anecdotes.[9] This is partly the consequence of more general problems that the area of intelligence studies is suffering from. In the first place, there is a general lack of theory within this discipline. It is thus not as common as in other academic disciplines, most notably the social sciences, to study intelligence from a theoretical framework.[10] Second, intelligence studies scholars fail in a spatial and temporal way to build on – and position their work vis-á-vis – the work of other and earlier scholars. Intelligence studies is a predominantly an Anglo-Saxon field of inquiry, and so the histories of intelligence and security services outside English speaking countries are studied to a much lesser extent, as is the literature in other languages.[11] In an intellectual sense, the failure to build on each other's work is even more problematic, as Stephen Marrin argues. Marrin's main point is that a lot of research is being done in the intelligence studies, but it fails to become 'cumulative', i.e. it fails to build on its own intellectual history. Researchers are not really debating each other's work, nor do they extensively reflect on the dominant insights in the field. Comparative studies are scarce.[12] Most studies, as Bob de Graaff argues, are of a descriptive nature and focus on a specific part of the intelligence practice, usually on a specific case, which is studied independent of (or not explicitly linked to) its international and national political context.[13]

Towards historians' greater involvement

Many authors addressing these shortcomings plea for advancing the theoretical underpinnings of the intelligence studies.[14] Theories may be important, but certainly not the only way forward in the intelligence studies. Although this social scientific answer to the 'academic deficit' of the intelligence studies may alleviate some of the observed problems, historians can bring something to the table too. Where social scientists seek to understand how intelligence and security services function in general, even 'a theory that can inform intelligence studies everywhere' around the world[15], historians can show how particular organizations have institutionalized, in which contexts, and how they operated the way they did. Historical research could also show why intelligence and security services function as they have done and still do in particular times and places. This enhances our understanding of the intelligence phenomenon in general, without losing relevant contextual factors out of sight.

In order to do so, however, intelligence historians have to contribute to intelligence studies in another way than they have so far.[16] Historians of intelligence have written very interesting books and articles on a broad range of particulars of the world of intelligence and security services, stretching from organizational histories to accounts of particular intelligence operations, but as is the case with

the intelligence studies discipline as a whole, they rarely analyze their findings in the light of common themes, problems, approaches, and broader questions.

The way forward within intelligence studies, is not solely social scientific – the answer does not lie exclusively in theorizing, as mentioned above – but is also of historical nature. Historical research can be of added value to our understanding of what intelligence is and does. In order to be relevant for fellow historians and for intelligence studies as a whole, however, intelligence historians should transcend the particulars of their specific research and relate their cases to broader themes and questions. They should reflect on what their archival findings *mean* and answer the question 'so, what?'. To understand how, a deeper reflection on the state of intelligence historiography is necessary.

As mentioned quite often in reflections on intelligence studies, it is well-known that intelligence and security services have been chosen as the object of academic research only recently. Intelligence studies have come into being since the famous Yale professor and intelligence analyst at the Central Intelligence Agency (CIA), Sherman Kent, published his 'Strategic intelligence for American world policy' in 1949.[17] The establishment of the in-house peer-reviewed academic journal 'Studies in intelligence' is described as another important step in the process of 'academization' of intelligence studies.[18] Kent was, however, predominantly interested in professionalizing the trade of intelligence analysis and in order to do so he more or less borrowed the academic practices from the social sciences.[19] He borrowed social scientific insights and practices to establish definitions, concepts, and theories for the intelligence studies.[20]

Professional historians (and political scientists) became involved only decades later. When in the 1970s publications on the role of SIGINT in the Second World War (ULTRA) appeared, and especially since the American year of intelligence (1975), citizens, journalists, and scholars became interested in intelligence and security services.[21] In 1984, nevertheless, the British historians Christopher Andrew and David Dilks described intelligence still as the 'missing dimension' of political and military history. In their book 'The missing dimension: governments and intelligence communities in the twentieth century', Andrew and Dilks argue that historians have largely ignored the role of intelligence and security service in many important historical events, thus omitting an important element in their analysis of decision and policy making.[22] In their attempt to explain where this neglect of the intelligence dimension stemmed from, Andrew and Dilks observed that many of their colleagues were rather hesitant to start doing academic research on intelligence and security services, because in books and movies espionage was depicted in an overly romantic, exciting, and heroic fashion. No one who considered him or herself as a serious, professional historian dared to be associated with this laughable topic, the two authors argued.[23]

More importantly, historians ignored intelligence and security services because they believed that secrecy rendered it impossible to do archival research. This,

however, was a misconception. Blaming contemporary historians for being spoiled – sources are abundantly available in modern times, especially from the twentieth century onwards – the two British authors point out that, although access to archives was indeed more problematic than in other branches of government, it was by no means impossible to study the archives of intelligence organizations. So even though official archives were inaccessible, intelligence documents have ended up elsewhere too. British politicians and high ranked civil servants, for example, regularly brought intelligence documents home, until the Cambridge Five spy ring was uncovered and they became much more security aware. The intelligence historian could therefore explore their personal archives, Andrew points out. The British Secret Intelligence Service furthermore worked in the interwar years under cover organizations, such as the Passport Control Office, the archives of which were accessible to the intelligence historian.[24]

Their call to historians to take this research seriously was picked up on only a few years later. An important catalyst was the fall of the Berlin wall in November 1989. In former communist countries, archives opened up for public use and historical research as a means of coming to terms with the dictatorial past, whilst in the West accountability and transparency were becoming more important. As a result, intelligence and security services began publishing (declassified) annual reports, and more importantly, intelligence archives became more accessible, amongst others in the United States and Great Britain.[25] The Dutch security service (*Binnenlandse Veiligheidsdienst* or BVD) transferred its archives of one of its predecessors, the transitional Bureau for national security (*Bureau Nationale Veiligheid*, BNV, which existed in 1945 and 1946) to the national archive in The Hague and published its official history in 1995.[26] More recently, intelligence documents from 1946-1952 and 1952-1989 were selected for transfer to the national archives, which has its limits at the same time. Due to the fact that operational information and third-party intelligence is not available to the researcher, the historian will find it difficult to do research on operational efficacy and intelligence liaison. The so-called 'zero files' (*nul-dossiers*), which contained the names and personal data of sources and agents, will never be transferred. The Dutch intelligence community actually has the right to destroy them, fearing that the willingness of sources to cooperate today would diminish if they learn that one day (even if the declassification date would be set a hundred and fifty years later) their names and backgrounds would become public.[27]

The body of knowledge, intelligence historiography, has nevertheless grown since the 1990s. Official histories of MI6[28] and MI5[29] have been published, and important journals such as *Intelligence and National Security* and the *International Journal for Intelligence and Counterintelligence* have been established[30], in the Netherlands (as a Dutch chapter of the *International Intelligence History Association*)[31] the *Netherlands Intelligence Studies Association* has been established, an association of former practitioners and academics, and at several universities research and

academic teaching programs on intelligence have developed, and so the body of knowledge – in terms of definitional debates, the study of intelligence failures, research on practices of oversight – is steadily growing.[32] Scholars in the intelligence studies have moved beyond the aim of fortifying the intelligence practice, and now study a broad range of themes within the field of intelligence and security.[33]

Intelligence historians, specifically, have published on a wide range of topics as well. The First World War remains a field of studies that can be explored more thoroughly,[34] whilst the Second World War has been studied more in-depth. The British codebreakers and their role in the interception of important German communication, as well as the infamous Pearl Harbor attack and the subsequent growth of the American intelligence apparatus have been the object of extensive historical research. The ensuing Cold War has been studied most intensively, although some events, such as the Cuban missile crisis of 1962 and the fall of the Berlin Wall in 1989, have attracted much more attention than other events. Ever since, the terrorist attacks of 9/11 and the American invasion in Iraq in 2003 have also been addressed by many contemporary historians.[35]

The missing dimension's missing dimension

Notwithstanding the growth of the body of knowledge, the literature on intelligence history shows several shortcomings. In a geographical sense, to begin with, much of the literature focuses on the Anglo-Saxon world, especially on Great Britain and the United States.[36] Although these are countries with a fascinating intelligence history, smaller countries such as Finland, Belgium, and Slovenia may be as interesting. Secret services outside the Western world have even been ignored to a larger extent.[37]

In a temporal sense, secondly, many historians have exclusively focused on the Cold War era and within this Cold War focus, some perspectives and activities have received substantially less attention. The intelligence activities of the Soviet Union outside the Western world, for example in Africa, have been largely neglected.[38] In addition, many historians have done research on the craft of espionage, more broadly on human intelligence (HUMINT) operations, whilst signals intelligence (SIGINT) has barely been studied.[39] Studying the role of SIGINT, however, may be worthwhile. Politicians tend to appreciate SIGINT more than HUMINT: SIGINT is a less perilous undertaking (no spies physically present in the object country), it is generally quickly available to them, it seems more objective than HUMINT, and it is often unique.[40] The National Security Agency (NSA) delivers the Black Book every 24 hours to the American president, containing the most important decrypts; Government Communications Headquarters (GCHQ) sends the prime minister and senior cabinet members a comparable Blue Book, and the Dutch prime minister has received SIGINT daily in the Green Edition (*Groene Editie*) for many years.[41]

A different kind of flaw in the historiography on intelligence and security services is the lack of research on the 'soft side' of intelligence and security. Many historians look into interesting intelligence operations of the past, as well as the organizations and their histories, but the views and social backgrounds of the employees of intelligence and security services, their mutual relationships, and their individual careers could be studied more in-depth, since these factors might influence the practice of intelligence analysis.[42] In addition, the public perceptions of intelligence and practices of oversight could be studied more extensively, in order to gain insight in the intelligence culture of a certain country – the institutional forms, cultural context, and social practices of intelligence and security.[43] Historical research should not only focus on what intelligence and security services have done in terms of activities, but also on how this was legitimized in a political and societal sense.[44]

Where, to present, the historiography has chronicled the organisational and operational history of the Dutch security services, the book 'Images of the enemy' (*Vijandbeelden*)[ii] presents the Dutch security services between 1912 and 1992 from a political, societal, and bureaucratic perspective, shifting to the interaction between the security services and their multi-facet environment they work in, in order to understand how this interaction influenced the threat and enemy perceptions, the organization, and the legitimacy of the Dutch Intelligence Community over time. This broad approach provides more insight in the way civil servants, politicians, journalists, and concerned citizens perceived of the intelligence and security services and to what extent they were able to exercise influence over its mandate, powers, tasks, and activities.[45]

The most important flaw in the intelligence historiography, however, is the lack of coherence. This argument applies to the intelligence studies as a whole, as Stephen Marrin also emphasized: scholars in this domain publish all kinds of studies, but the body of literature fails to be cumulative and does not build on its own intellectual history. It is not common practice for intelligence scholars to interact, debate, and extensively respond to each other's work, nor has a common set of questions been developed.[46]

This holds true for intelligence historians specifically. As mentioned before, a large number of historical articles and books are of descriptive nature and focus on stand-alone cases and do not pay much attention to the societal and (international) political context. Comparative studies are rarely conducted.[47] Scholars tend to prefer exciting intelligence operations over seemingly duller institutional comparisons of organizations. And because of that, Philip Davies argues, scholars in this domain wrongly tend to regard intelligence and security services as exotic and unique organizations, to be studied in isolation. To a large extent, intelligence and security services are normal government organizations,

ii Book published in Dutch by the author – original title

and therefore they have been integrated into government bureaucracies for decades. They interact with less arcane parts of governments and in terms of management, reporting, and culture they resemble 'normal' governmental organizations to a large extent. The lack of attention for this bureaucratic character of intelligence and security services is what Davies describes as the missing dimension's missing dimension.[48]

Prospects for the future

In order to become more than a catalogue of interesting organizational and operational histories, historians of intelligence will need to adapt. In the first place, the discipline as a whole would benefit from more historians becoming involved in research on intelligence and security services.[49] On the one hand, intelligence historians could make their colleagues in, for example, political history and the history of social movements aware of the intelligence dimension of their topics. They could sensitize them and encourage them to be aware of a possible intelligence angle to their topics. On the other, it would be constructive for the discipline of intelligence history if historians from different backgrounds poured into the intelligence and security domain. It seems that many historians are still hesitant to become involved in research on intelligence and security – possibly because of the exact reasons Andrew and Dilks already presented in the 1980s: an overly romantic view of espionage and the idea that sources are lacking. In the Netherlands, a small country of course, no more than a handful of academics is studying the history of intelligence and security.

A first improvement to the field of intelligence history, thus, would be that more historian become involved. When more academics enter the field, they bring with them insights from other historical disciplines, such as political, social, and economic history, and enrich and enhance the central problems and approaches within the historical research on intelligence. They could contribute to formulating a set of core problems and related questions. More historians could also help to professionalize the historical discipline of the intelligence studies by asking methodological questions. Historians are pre-eminently trained to ask heuristic and epistemological questions, which are especially valuable in the domain of intelligence and security. Knowing where to find documents and knowing what you can and cannot claim on the basis of these documents, is of great value in a field of historical research where sources are scarce and manipulation and deception is common.[50] This could help intelligence historians to more structurally reflect on the methodology of their work and exchange views on and experiences with doing research in the archives of intelligence and security services. A discussion about the practice of applying internal and external source criticism, not only in terms of access to sources, but also in terms of interpretation of intelligence documents, would provide the field of intelligence history with a broader academic basis.[51]

Second, to bring the field of intelligence history to the next level, historians could draft a research agenda. In itself this idea is not new. Other authors have also argued to restore the geographical balance by doing more research on other countries than the United States and Great Britain, most notably the non-Western world.[52] From the temporal perspective, of course the Cold War remains a very interesting and in many respects crucial era to be researched[53], but in addition earlier periods of time should be the subject of historical inquiry as well. Finally, the role of SIGINT needs to be addressed more extensively as well.[54]

What is, however, more important than a fixed list of topics, is that intelligence history needs to become more cumulative. In order to do so, in the words of John Lewis Gaddis they 'have to devote less time to cataloguing operations and expend more effort in demonstrating how it made things different'.[55] To this aim, historians should do more comparative research and should try to relate their empirical findings to central themes, which could also be addressed by other intelligence historians. One way to take this to the next level is to look at 'intelligence systems'[56] or 'intelligence cultures' from an historical perspective, terms respectively coined by Michael Warner and Philip Davies, which could be used as a lens to study particular cases, in particular places and specific timeframes, and could therefore be used to analyze the meaning of a particular case in the light of a broader theme, problem, or question, which is already addressed in the literature. Such an exercise helps us to strengthen our understanding of the way intelligence and security services are formed and transformed in different contexts.

History's contribution to strengthening intelligence cultures

The term 'intelligence culture' was coined by the British scholar Philip Davies. An intelligence culture comprises the institutional forms, cultural context, and social practices of intelligence and security. This corresponds with a broader trend within international relations and the security studies, which increasingly sheds light on norms and identity politics.[57] Davies observed that, although in many Western countries the essential functions of intelligence and security services are the same – they all to a larger or lesser extent collect, process, and analyze specific information, which they disseminate to other branches of government who can act upon it –, the intelligence practice can be notably different in different countries. Not only are for example the American and British organizational, judicial, and institutional structures markedly different, but also the convictions, concepts, values, and norms that lie behind the customs and practices of the people and organizations involved can be rather different. As a result, not only the institutional arrangements, but the essential meaning of 'intelligence' is different in both countries, Davies argues.[58]

Philip Davies, Kevin O'Connell[59], Michael Warner[60] and Isabelle Duijvestein have therefore advocated that cultural aspects should be higher on the research agenda

of the intelligence studies.[61] Bob de Graaff and James Nyce have edited a book on European intelligence cultures, exploring in quite a number of (also East and Central) European countries which cultural and social variables help explain 'how intelligence processes are conducted and legitimized in a particular country'.[62]

The concept of national intelligence cultures is a useful instrument for the discipline of intelligence history. It serves to study the historical formation and transformation of intelligence cultures in different times and places, and allows historians to understand changing and different functions and meanings of intelligence.[63] Historians should answer the question 'so, what?' by zooming out in their analysis of their particular cases. To what extent did the operation under study reflect a broader intelligence culture, in what sense what did it contribute to the national security policies? More broadly, historians should seek an answer to questions, such as:

- What difference did the intelligence and security services make?[64]
- Who, in the specific country that is studied, is politically responsible for the intelligence and security services, who manages them, who gets to set their priorities and requirements, and who receives their reports and briefings?
- To what extent does new archival research shed new light on prevailing insights?
- To what extent should the classics be amended, altered, or rewritten altogether?[65]
- What was the added value of intelligence in a certain situation, how did people go about using or ignoring it?
- What role did it eventually play?
- How did politicians perceive of their secret services; to what extent did they think their activities were useful to them? And if they deemed them useful, then in what way?
- Why did, for example, Margaret Thatcher rely heavily on the security service and the secret intelligence service for her decision making, whilst Helmut Kohl was mistrustful of his intelligence apparatus? And how to account for the fact that Mitterrand encouraged his intelligence services to conduct technical operations against other heads of state, whilst Chirac fired two intelligence chiefs on the day he became president?[66]

These kinds of questions should be addressed, even when researching very particular intelligence operations from a distant past, in order to improve our understanding of how societies and states relate to their intelligence and security services and how intelligence practices develop over time. To this purpose, it would be worthwhile to draft a list of core questions, comparable to the questions

suggested above, which of course can be amended and changed over time. These could focus on intelligence and security services as bureaucratic organizations: find out with whom they frequently interacted, what kind of reports they produced and who were the recipients of those reports and briefings, which political and bureaucratic management styles prevailed, what kind of opinions members of parliament had of their secret services and how citizens perceived the added value of intelligence and security services.[67] The intelligence historian should no longer solely try to uncover the missing dimension, but he or she should try to shed light on the ideological, political, cultural, and social practices associated with intelligence and security.[68]

History and the intelligence analyst

This 'academization' of intelligence history does not only benefit (professional) historians; it could be an advantage to intelligence analysts too. Historical consciousness, for one, is needed to understand the development of the trade of intelligence analysis. As pointed out by John H. Hedley, the development of intelligence analysis as a trade was the product of the enveloping Cold War: with the rise of the American 'national security state' came a need for 'global information', which 'would need to cover not just enemy military forces but also political and economic developments worldwide' – a need that drove the institutionalization of intelligence analysis and the professionalization of the trade.[69]

More importantly, however, history can benefit intelligence analysts in terms of content. This is not standing practice, however. The renowned intelligence historian Christopher Andrew argues that we, humans in the present – and with us current intelligence analysts –, suffer from a 'delusion' that convinces us that 'what is newest is necessarily most advanced'. Andrew challenges analysts therefore to learn from 'longer-term intelligence experience' instead.[70]

Analysts themselves agree that studying history can help improve the quality of their analysis. As a former CIA analyst with forty years of experience put it:

> 'An understanding of history and culture is key to coming to grips with the assumptions that underpin much of our analysis. And I am not talking about our history and culture, but the history and culture of the countries we work on *as the people and leaders of those countries understand them*. Every analyst—regardless of discipline or role—needs a deep appreciation of how a people see themselves, their historical ambitions, and their grievances. For analysts focused on foreign leaders, or politics, or economics, it is essential that they understand how power is acquired, the preferred way of exercising power, and the acceptable and unacceptable uses of power, as well as the defining life experiences of the key actors in the countries they specialize in.'[71]

The same applies to counterintelligence, a domain in which historical spy cases can and have been very useful to understand the modus operandi, intentions, and capabilities of opposing intelligence services. In the Netherlands, for example, the post war counterintelligence and security service, lacking an intelligence position on Soviet intelligence activities in the Netherlands, started out with reading everything the authorities had written about agent networks run by Soviet intelligence services before the Second World War. But in other domains lessons can be learned from specific situations as well, Erik J. Dahl argues.[72] For these reasons, history – and more specifically historical cases – seem to play an important role in intelligence analysis, also in their training programs.[73]

Besides providing relevant 'historical facts', an historical way of thinking might be beneficial to intelligence analysis as well. Historical research benefits intelligence analysts by helping him or her to 'discern what the story is, instead of what the problem is; it helps to determine the who, what, when, where, how and the why of a narrative'. At the same time, there are epistemological impediments to history's use to the intelligence analyst: history is multi-interpretable, it is uncertain (and historians can be wrong), and it is incomplete.[74] The same applies to intelligence analysis as a whole, in which analysts continuously run the risk of inferring 'direct cause-and-effect relationships' in their estimates, where reality turns out to be more complex, Cyrus H. Peake argues. In his view, an analyst

> 'with historical perspective will be on guard against the error of extending a narrow unilinear analysis of a current situation into a general forecast, of automatically extending, for example, the analysis of an economic situation to cover the political and psychological future, on the mistaken assumption that economic laws determine the course of human affairs.'[75]

In other words, the intelligence analyst with an historical mind-set could write better analyses. Historians such as Peter Jackson support this argument, pointing out that the professional skills that historians have developed can be useful to intelligence analysts too. Historians, just as intelligence analysts, are trained to apply thorough source criticism and they continually ask methodological and epistemological questions: they reflect on the steps in the argument, the context and trustworthiness of knowledge. The historian knows that nothing speaks for itself, and that 'how it really was' depends on one's perspective on past events – skills that the intelligence analyst can use as much as the professional historian.[76]

For this reason, the way forward for intelligence historians might also benefit intelligence analysts. An example is the concept of intelligence cultures that intelligence historians might use to reflect on the findings of their particular cases. For intelligence analysts, this concept might show, for example, that 'intelligence analysis' might mean something else in Belgium than in the Netherlands. Philip Davies has argued in this light, for example, that the British characteristic of

collegiality might make British analysts fall back 'on common assumptions and institutional orthodoxies in formulating assessments'. American intelligence analysis might on the other hand be influenced by turf wars and aversion of compromise, presenting their consumers with 'a plurality of opinions', even resulting in 'analysis paralysis'.[77]

Conclusion

Historians studying intelligence and security services should, to put it briefly, expand their horizon. They should broaden the scope of their research, discuss the methodological basis of this specific field of interest more extensively, and draft a research agenda and, more importantly, a core set of questions that allows them to discuss each other's findings, no matter how different they are in temporal and geographical terms. Only then it will be possible to improve our common understanding of what intelligence and security means in practice, and how it is being put into tangible and concrete organizations, activities, words, and deeds.

In the Dutch case, presented in the introduction, in which the institutionalization of a civil security service went hand-in-hand with an intensive discussion, historians should reflect on these arguments as a means to understand the formation and transformation of the Dutch 'intelligence culture'. Historians should explore why the military officers and police inspectors involved argued for or against the establishment of such a service, how the resistance to Fabius' plans fitted within the broader political and bureaucratic culture of the Netherlands at the time. It should be addressed what the added value of this new instrument for the state would be, what the security service practically did, and who it benefitted in terms of information advantage. It could also be asked to what extent this influenced the development of intelligence analysis, which in the Netherlands only came to fruition in the Cold War. All this can then be linked to one of the core questions of the broader research agenda for intelligence historians, such as: why, and how, do states institutionalize and maintain intelligence organizations? By trying to answer that, insights from the Dutch case are then made accessible for future research on comparable cases. This would make the historiography on intelligence and security services much more cumulative, which would be a major step forward.

This applies to academic historians, studying the history of intelligence and security services, but also to intelligence analysts practicing the trade today. Intelligence analysts who know how to benefit from historical insights, applying 'lessons learnt' in their analysis, can prevent cognitive bias and can contribute to qualitatively better analysis. Official historians could help intelligence analysts, as long as these historians have full access, are free to 'make whatever deductions consistent' with their archival findings, and that they deal with the entire intelligence cycle.[78] There is, to conclude, a broader interest to take the

academic study of intelligence history more seriously. Time has come to care about the future of intelligence history. Instead of 'painstakingly piecing together lost worlds from pottery fragments, scraps of manuscripts, and faded inscriptions on broken steles', as Michael Warner puts it, intelligence historians can now take their field of inquiry tot the next level.[79] Intelligence historians should always ask themselves what their sources tell them about a phenomenon, topic, or theme that is more broadly researched in the intelligence studies. Only then will future research be more beneficial to our general understanding of this complex world of intelligence and security.

Endnotes:

*01_* National Archives the Netherlands, Kopiecollectie [copied collection] De Meijer, 2.04.53.21, inv.nr. 17, Dagboek [Diary] Van Woelderen, 13 november 1918 en 17 november 1918.

*02_* C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie, 1912-1992* [Images of the enemy. Dutch security services and democracy, 1912-1992] (Amsterdam: Boom 2016); C.W. Hijzen, 'The Perpetual Adversary. How Dutch Security Services Perceived Communism (1918-1989)', *Historical Social Research* 38 (1) 2013: 166-199.

*03_* C.W. Hijzen, *Vijandbeelden*.

*04_* R.J. Aldrich, The hidden hand. Britain, America and Cold War secret intelligence (Woodstock and New York 2002) 5.

*05_* P.J. Davies, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs*, October 2004, 17, 3, 495-520, there 498, 517.

*06_* P.J. Davies, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs*, October 2004, 17, 3, 495-520, there 500.

*07_* P. Davies, Ideas of intelligence: divergent national concepts and institutions, *Harvard International Review*, 24, 3, fall 2002, 62-66, there 66.

*08_* One of the first authors to observe this was Glenn P. Hastedt: G.P. Hastedt, 'Towards the comparative study of intelligence', *Conflict Quarterly*, 11, 3 (Summer 1991) 55-72. More recently it was noted by, amongst others, Peter Gill: P. Gill, '"Knowing the Self, knowing the Other": the Comparative Analysis of Security Intelligence', in: L.K. Johnson ed., *Handbook of Intelligence Studies* (New York, NY and London 2007) 82-90, there 82.

*09_* E.g. R.J. Aldrich, 'Grow your own. Cold War intelligence and history supermarkets', *Intelligence and National Security* 17, 1 (2002) 135- 152.

*10_* E.g. D. Kahn, 'An historical theory of intelligence', P. Gill, S. Marrin en M. Phythian ed., *Intelligence Theory: Key Questions and Debates* (London en New York, NY 2009) 4-5: 4; P. Gill, 'Theories of Intelligence: where are we, where should we go, and how should we proceed?' in: P. Gill, S. Marrin en M. Phythian ed., *Intelligence Theory: Key Questions and Debates* (London and New York, NY 2009) 208-226, there 210-213.

*11_* E.g. 'P.H.J. Davies en K.C. Gustafson, 'An agenda for the comparative study of intelligence: yet another missing dimension', in: P.H.J. Davies en K.C. Gustafson (red.), *Intelligence elsewhere. Spies and espionage outside the Anglosphere* (Washington 2013) 3-12, there 8-9.

12_ S. Marrin, 'Improving intelligence studies as an academic discipline', *Intelligence and National Security* 22 (October 2014), 1-14, there 4.

13_ B.G.J. de Graaff, *De ontbrekende dimensie: intelligence binnen de studie van internationale betrekkingen* [The missing dimension: intelligence in the study of international relations] (2 March 2012) (Utrecht 2012) 13-14.

14_ E.g. M.Warner, 'Building a theory of intelligence systems', in: G.F. Treverton en W. Agrell (red.), *National intelligence systems. Current research and future prospects* (New York 2009) 11-37: 11-12; P. Gill, 'Theories of intelligence: where are we, where should we go and how might we proceed?', in: Peter Gill, Stephen Marrin, and Mark Phythian, *Intelligence theory: key questions and debates* (London and New York 2009) 208-226, there 222-223.

15_ Cf. P. Gill, 'Theories of intelligence: where are we, where should we go and how might we proceed?', in: Peter Gill, Stephen Marrin, and Mark Phythian, Intelligence theory: key questions and debates (Londen en New York 2009) 208-226, there 223.

16_ Cf. R. Gerald Hughes, 'Of revelatory histories and hatchet jobs: propaganda and method in intelligence history', *Intelligence and National Security*, 23, 6, 2008, 842-877.

17_ S. Kent, Strategic Intelligence for American World Policy (Princeton, NJ 1949).

18_ H.P. Ford, 'A tribute to Sherman Kent', *Studies in Intelligence*, 24, 3, 1980.

19_ J.J. Wirtz, 'The American approach to intelligence studies' in: L.K. Johnson ed., *Handbook of Intelligence Studies* (New York, NY and London 2007) 28-38, there 32-33.

20_ E.g. G. de Valk, Dutch Intelligence - Towards a Qualitative Framework for Analysis: With Case Studies on the Shipping Research Bureau and the National Security Service (BVD) (Groningen: dissertation 2005) 10-11.

21_ H.C. Deutsch, 'The historical impact of revealing the Ultra secret', *Parameters: journal of the US Army Journal*, VII, 3, 1977, 16-32; F.H. Hinsley en A. Stripp, *Codebreakers: the inside story of Bletchley Park* (Oxford: Oxford Universirty Press 1994); H. Rositzke, *The CIA's secret operations: espionage, counterespionage, and covert action* (Boulder 1977).

22_ C. Andrews and D. Dilks, The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century (London 1984).

23_ Andrew and Dilks, The *Missing Dimension*, 1-3.

24_ Andrew and Dilks, The *Missing Dimension*, 4-5; P. Jackson, 'Introduction: enquiries into the 'secret state' in: R.G. Hughes, P. Jackson, en L. Scott ed., *Exploring intelligence archives: enquiries into the secret state* (New York, NY 2008) 1-10, there 5-6.

25_ L. Scott and P. Jackson, 'The Study of Intelligence in Theory and Practice', *Intelligence and National Security* 19:2 (2004) 139-169, there 152, 155, 164-165.

26_ D. Engelen, *De geschiedenis van de Binnenlandse Veiligheidsdienst* [The history of the Domestic Security Service] (Den Haag 1995); National Archives the Netherlands, Bureau Nationale Veiligheid, toegangsnummer 2.04.80.

27_ National Archives the Netherlands, Archief van de Centrale Veiligheidsdienst (1946-1949) en de Binnenlandse Veiligheidsdienst (1949-1952) van het Ministerie van Binnenlandse Zaken: open dossiers, inventarisnummer 2.04.12.

28_ K. Jeffery, The *Secret History of MI6 1909-1949* (New York, NY 2010).

29_ C. Andrew, *The Defence of the Realm. The Authorized History of MI5* (London: Penguin 2009).

30_ C. Andrew, 'Reflections on Intelligence Historiography Since 1939' in: G. Everton and W. Agrell ed., *National intelligence systems: current research and future prospects* (New York, NY 2009) 38-57, there 50-51; De Graaff, 'De ontbrekende dimensie', 6-11.

31_ Internet: http://intelligence-history.org.

32_ M.M. Lowenthal, *Intelligence: from secrets to policy* (Washington, DC 2009) 1-2; De Valk, *Dutch Intelligence*, 8-9; Scott and Jackson, 'The study of intelligence', 141-43; De Graaff, 'De ontbrekende dimensie', 11-14.

33_ Wirtz, 'The American approach', 32-33; S. Marrin, 'Intelligence analysis and decision-making: methodological challenges' in: P. Gill, S. Marrin ad M. Phythian (ed.), *Intelligence Theory: Key Questions and Debates* (London and New York 2009) 131-150; De Valk, *Dutch Intelligence*, 32-39; L.K. Johnson, 'Preface to a theory of strategic intelligence', *International Journal of Intelligence and Counterintelligence* 16 (2003) 638-663; Scott and Jackson, 'The study of intelligence', 144; S. Berman, 'Ideas, norms, and culture in political analysis (review article)', *Comparative Politics*, 33.2 (2001) 231-250, there 235.

34_ D. Larsen, 'Intelligence in the First World War: the State of the field', *Intelligence and National Security* 26 (October 2012) 1-26.

35_ R. Wohlstetter, *Pearl Harbor, Warning and Decision* (Stanford 1962); L.K. Johnson and A.M. Shelton, 'Thoughts on the state of the intelligence studies: a Survey Report', *Intelligence and National Security* 28, 1, 2013, 109-120, there 112. E.g.. B. Latell, *Castro's secrets. The CIA and Cuba's intelligence machine* (New York, NY 2012); P.R. Pillar, *Intelligence and U.S. foreign policy. Iraq, 9/11, and misguided reform* (New York, NY 2011); A.H. Cordesman en A.A. Burke, *Intelligence failures in the Iraq War* (Washington, DC 2003); R. Jervis, *Why intelligence fails. Lessons from the Iranian Revolution and the Iraq War* (Ithaca en London 2010); O. Riste, 'The intelligence-policy maker relationship and the politicization of intelligence' in: G. Everton en W. Agrell (eds.), *National intelligence systems: Current research and future prospects* (New York 2009) 179-209.

36_ Johnson and Shelton, 'Thoughts on the state of the intelligence studies', 113; P. Gill, 'Theories of intelligence: where are we, where should we go, and how should we proceed?' in: P. Gill, S. Marrin en M. Phythian ed., *Intelligence theory: key questions and debates* (London and New York, NY 2009) 208-226, there 213-219.

37_ P.H.J. Davies and K.C. Gustafson, 'An agenda for the comparative study of intelligence: yet another missing dimension', in: P.H.J. Davies en K.C. Gustafson ed., *Intelligence elsewhere: spies and espionage outside the Anglosphere* (Washington, DC 2013) 3-12, there 8-10.

38_ Johnson and Shelton, 'Thoughts on the state of the intelligence studies', 113-114; C. Andrew, 'Reflections on intelligence historiography since 1939', in: G. Everton en W. Agrell (eds.), *National intelligence systems: current research and future prospects* (New York 2009) 38-57, there 46.

39_ Andrew, 'Reflections on Intelligence Historiography since 1939', 38-44.

40_ M. Aid and C. Wiebes, 'Introduction on the importance of SIGINT in the Cold War' in: Idem (eds.), *Secrets of signals intelligence during the Cold War and beyond* (London 2001) 1-24.

41_ Aid and Wiebes, 'Introduction on the importance of SIGINT in the Cold War', 6; De Graaff and Wiebes, *Villa Maarheeze*, 280-282.

42_ Johnson en Shelton, 'Thoughts on the state of the intelligence studies', 113.

43_ H.J. Davies, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs* 17.3 (2004).

44_ B. de Graaff and J.M. Nyce, 'Introduction', in: idem, *The handbook of European intelligence cultures* (Lanham 2016), I-XLVI, XXXIII.

45_ C.W. Hijzen, *Vijandbeelden. De veiligheidsdiensten en de democratie, 1912-1992* (Amsterdam 2016).

46_ S. Marrin, 'Improving intelligence studies as an academic discipline', *Intelligence and National Security* 22 (October 2014) 1-14, there 4.

47_ P. Gill, '"Knowing the Self, knowing the Other": the comparative analysis of security intelligence', in: L.K. Johnson ed., *Handbook of intelligence studies* (New York, NY and London 2007) 82-90; De Graaff, 'De ontbrekende dimensie', 13-14.

48_ P. Davies, 'Intelligence and the machinery of government: conceptualizing the intelligence community', *Public Policy and Administration* 25.1 (2010) 29-46, there 42.

49_ P. Jackson, 'Introduction: enquiries into the 'secret state' in: R.G. Hughes, P. Jackson, en L. Scott ed., *Exploring intelligence archives: enquiries into the secret state* (New York, NY 2008) 1-10.

50_ Jackson, *Enquiries*, 3.

51_ E.g. P. Tosh, *The pursuit of history* (3rd edition: Harlow 2000) 58-69.

52_ P.H.J. Davies and K.C. Gustafson, 'An agenda for the comparative study of intelligence: yet another missing dimension', in: P.H.J. Davies en K.C. Gustafson ed., *Intelligence elsewhere: spies and espionage outside the Anglosphere* (Washington, DC 2013) 3-12.

53_ R.J. Aldrich, The hidden hand. Britain, America and Cold War secret intelligence (New York 2001) 1-16.

54_ C. Andrew, 'Reflections on intelligence historiography since 1939', in: G. Everton en W. Agrell (eds.), *National intelligence systems: current research and future prospects* (New York 2009) 38-57.

55_ Quoted in: R.J. Aldrich, 'Grow your own. Cold War intelligence and history supermarkets', *Intelligence and National Security* 17, 1, 2002, 135-152, there 140-141.

56_ K.M. O'Connell, 'Thinking about intelligence comparatively', Brown Journal of World Affairs XI, 1, 2004, 189-199, there 189-190; M. Warner, 'Building a theory of intelligence systems', in: G.F. Treverton en W. Agrell (red.), *National intelligence systems. Current research and future prospects* (New York 2009) 11-37, there 14, 26-35.

57_ P. Hall en Rosemary Taylor, 'Political science and the three new institutionalisms', *Political Studies* vol. 44, 4, December 1996, 936-957, there 938-393; L. Jepperson, A. Wendt en P.J. Katzenstein, 'Norms, identity, and culture in national security', in. P.J. Katzenstein, *The culture of national security: norms and identity in world politics* (News York 1996) 33-75, there 42-43.

58_ P. Davies, Ideas of intelligence: divergent national concepts and institutions, *Harvard International Review*, 24, 3, fall 2002, 62-66.

59_ K.M. O'Connell, 'Thinking about intelligence comparatively', Brown Journal of World affairs XI, 1 (2004) 189-199, there 189-190; P. Gill, '"Knowing the self, knowing the other" The comparative analysis of security intelligence', in: L.K. Johnson (ed.), *Handbook of intelligence studies* (New York/Londen 2007) 82-90.

60_ M.Warner, 'Building a theory of intelligence systems', in: G.F. Treverton en W. Agrell (eds.), *National intelligence systems. Current research and future prospects* (New York 2009) 11-37.

61_ I. Duijvestein, 'Intelligence and strategic culture. Some observations', *Intelligence and National Security* 26, 4, 2011, 521-530.

62_ B. de Graaff and J.M. Nyce, 'Introduction', in: idem, *The handbook of European intelligence cultures* (Lanham 2016), I-XLVI, XXXIII.

63_ P. Gill, '"Knowing the Self, knowing the Other": the Comparative Analysis of Security Intelligence', in: L.K. Johnson ed., *Handbook of intelligence studies* (New York, NY and London 2007) 82-90.

64_ Special Issue: "Intelligence in the Cold War: what difference did it make." *Intelligence*

and National Security 26, 6, December 2011.

65_ We could choose a few handbooks, such as: L.K. Johnson ed., *Handbook of Intelligence Studies* (New York, NY and London 2007) and L.K. Johnson (ed.), *The Oxford handbook of national security intelligence* (Oxford 2010), but also historical overviews such as P. Knightley, *The Second Oldest Profession. The Spy as Bureaucrat, Patriot, Fantasist and Whore* (Londen/Sydney 1987) and J.T. Richelson, *A century of spies: intelligence in the twentieth century* (New York 1995).

66_ C. Andrew, 'Reflections on Intelligence Historiography since 1939', in: G. Everton en W. Agrell ed., *National Intelligence Systems: Current Research and Future Prospects* (New York, NY 2009) 38-57: 51-52.

67_ Marrin, 'Improving Intelligence Studies', 10-14; E. Braat, 'Recurring tensions between secrecy and democracy: arguments about the security service in the Dutch parliament, 1975–1995', *Intelligence and National Security* 8, June 2015.

68_ Jackson, 'Introduction: enquiries into the "secret state"', 3.

69_ J.P. Hedley, 'The evolution of intelligence analysis', in: R.Z. George and J.B. Bruce, *Analyzing intelligence: origins, obstacles, and innovations* (Washington D.C. 2008) 19-34, there 19.

70_ C. Andrew, 'Intelligence analysis needs to look backwards before looking forward', *History and Policy*, 1 June 2004. Internet: http://www.historyandpolicy.org/policy-papers/papers/intelligence-analysis-needs-to-look-backwards-before-looking-forward.

71_ M. Petersen, 'What I learned in 40 years of doing intelligence analysis for US foreign policy makers. In the first person', *Studies in intelligence*, 55, 1, March 2001. Internet: https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-55-no.-1/what-i-learned-in-40-years-of-doing-intelligence-analysis-for-us-foreign-policymakers.html.

72_ Erik J. Dahl (2017) Getting beyond analysis by anecdote: improving intelligence analysis through the use of case studies, Intelligence and National Security, 32:5, 563-578.

73_ Joseph Caddell Jr. & Joseph Caddell Sr., 'Historical case studies in intelligence education: best practices, avoidable pitfalls,' *Intelligence and National Security*, 32, 7, 207, 889-904.

74_ Paper E. Torres, *The limitations of history to the field of intelligence*, 14 February 2014. Internet: http://www.e-ir.info/2014/02/14/the-limitations-of-history-to-the-field-of-intelligence/#_ftn2.

75_ Cyrus H. Peake, 'History's role in intelligence estimating', *Studies in Intelligence* 3, Winter 1959. Internet: https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol3no1/html/v03i1a07p_0001.htm.

76_ P. Jackson, 'Introduction: Enquiries Into the 'Secret State' in: R.G. Hughes, P. Jackson, en L. Scott ed., *Exploring Intelligence Archives: Enquiries into the Secret State* (New York, NY 2008) 1-10: 5-6.

77_ P.J. Davies, 'Intelligence culture and intelligence failure in Britain and the United States', *Cambridge Review of International Affairs*, October 2004, 17, 3, 495-520, there 499.

78_ Paper Cletus Subetiq Nachelle, *Historical aspects of intelligence analysis* (20 September 2013).

79_ M. Warner, 'Documenting the history of intelligence history. Review essay of R. Gerald Hughes, Peter Jackson and Len Scott (eds), *Exploring intelligence archives: enquiries into the secret state* (London: Routledge 2008)', *Intelligence and National Security*, 24, 3, juni 2009, 458-463, there 458.

National Strategic Intelligence and Competitive Intelligence: How a Comparative View and Mutual Learning Can Help Each ?

Avner Barnea[i]

Abstract

National strategic intelligence and competitive intelligence seem to be two different disciplines. So far, research has focused on these two fields, national intelligence and competitive intelligence separately, without any attempt to benchmark from one field to the other. However, these two fields have a lot in common. In both government and competitive intelligence, intelligence inputs are embedding in the process of decision support system. One of the options emerging from comparing intelligence performance in both fields is the possibility to use accumulated experience in the business field to improve intelligence practice in national security context and vice versa through mutual learning. One particularly interesting aspect is the comparison between intelligence failures in both areas and how they can be prevented and whether any of these fields can be learned from the experience of other to improve performance.

***Keywords*:** national intelligence, strategic intelligence, national security, competitive intelligence, market intelligence, intelligence failures.

i School of Business, Netanya Academic College, National Security Studies Center, University of Haifa, Israel. Email: avnerpro@netvision.net.il .

Introduction[ii]

Significant strategic surprises are common both in the political-security sphere and in the business space. The Arab Spring (2011) in Egypt, Tunis, Yemen and Syria against the governments and rulers of these countries, demonstrated the far-reaching consequences of the strategic surprise in the security field. As for the competitive private sector, the strategic surprises of Nokia, the "world's mobile communications leader" with the arrival of Apple's iPhone (2007), and the blow of Kodak as a result of the company missing the digital revolution, led to their collapse. It is only natural that those planning a strategic move do all they can to bring it to surprise, while those who are charged with thwarting the opponent's strategic moves try their best to prevent surprise (Barnea, 2015).

According to the Strategic and Competitive Intelligence Professionals Association – SCIP (http://www.scip.org/), competitive intelligence is the process of legally and ethically gathering and analyzing information about competitors and the industries in which they operate in order to help the organization make better decisions and reach its goals. Competitive intelligence was introduced and became institutionalized in the 1980s, and more so since the second half of the 1990s. It was strongly influenced by studying the relevant experience acquired from government intelligence together with outstanding inputs from the business sector (Walle, 2001). One of the factors that drove the progress of intelligence in business forward was Michael Porter's pioneering book "Competitive Strategy" (Porter, 1980), which was one of the most influential works in the field of business strategy. While the information revolution became significant in business since the end of 1990's, the dynamic changes in the competitive environment transformed competition globally, and have pushed forward a comprehensive research and academic study in competitive and marketing intelligence, (Prescott, 1999; Tianjiao Qui. 2008; Vedder and Guynes, 2000; Dishman and Calof, 2008; Wright and Calof, 2006).

Although national strategic intelligence and competitive intelligence appear to be two unrelated fields, the ways in which challenges are addressed in each field are rather similar: they are largely depended on early-warning capabilities (Miscik, 2017; Gilad, 2004; Grabo, 2004); decision-makers having a close interface with intelligence expect to learn about threats and opportunities in advance. In this context, it is not surprising that in recent years, academic research in national, competitive and marketing intelligence has demonstrated that it is possible to perform a comparative analysis of the two fields (government and business) and identify possible parallels between them.

---

ii This article is an extended version of a paper that the author has previously published on the website of the Strategic and Competitive Intelligence Professionals Association – SCIP. The content of the paper was made available for limited dissemination in the online Competitive Intelligence Magazine, Vol. 16, No. 3, July - September, 2013.

One particularly interesting aim of this article is to compare historical intelligence failures in both areas and investigate if they could have been prevented and whether or not any of these fields can learn from the experience of each other to improve performance. The core argument in this paper is that in both intelligence fields, government and business, it is the intelligence product supporting the decision-making process that addresses and deals with changes in the external environment determined by existential threats to national security or business competitors. Consequently, both fields have room for improvement that could be achieved through a cross-functioning study. Nevertheless, although both judgments and choices are subject to common biases in the processing of information, which may lead to further errors made by decision-makers, this issue seems to be better researched in the business sector than in governmental organizations. (Sage, 1990; Kahneman and Tversky, 1984; Busenitz and Barney, 1997).

This qualitative research is based on a review of the existing literature on both competitive intelligence and government (strategic) intelligence. Building upon his findings, the author will then present which and how best practices can be applied to each field of intelligence. In addition, the purpose of this study is to show that mutual learning from each field can improve the quality and capacity of intelligence products to understand and address complex situations and support more effectively the decision-making process.

Similarities between government and competitive intelligence

A visible similarity between both government intelligence and competitive intelligence is that they both function based on the "intelligence cycle" (Johnston and Johnston, 2007; Omand, 2010). This is a systematic process of five steps ensuring that intelligence activities carry out under checks and balances. The intelligence cycle is a closed loop; feedback has to be received from decision-makers and revised intelligence requirements need to be issued to make sure that the intelligence product is fulfilling their needs.

However, navigating deeper into the subject, it appears that similarities between intelligence failures experienced in government and in the business field represent five major areas (Barnea, 2015):

1. Gathering ability: usually there is no shortage in information as these capabilities have developed considerably in recent years.
2. Noisy information environment: there are struggles with receiving and classifying information, even prior to the analysis stage, due to large amounts of unclear and sometimes contradicting information.
3. Organizational difficulties and lack of cooperation: failures which are derived from the structural complexity of organizations, as well

as inter- and intra-organizational competitiveness, affect cooperation and lead to the ineffective and inefficient use of vital intelligence.

4. Intelligence-policy relationship: the relationship dynamics may cause estimates to be biased due to the innate desire to please the policy/decision-maker. In addition, the dysfunctional relationship between intelligence and policy may even prevent intelligence analysts from sending and receiving intelligence to and from decision-makers in order to prevent a conflict between the desired policy and the intelligence entities.
5. The literature focuses on the intelligence analysts' failures.

The business world adopted the intelligence practices derived from government intelligence and applied them to its needs after making adequate modifications. However, the lack of resources which are allocated to fulfill competitive intelligence needs in corporations makes its scope more limited, and therefore, leads to a smaller number of issues (called Key Intelligence Topics – KITs) and the processing of less information. However, from its very beginning, competitive intelligence was not limited to only tracking threats from competitors or monitoring significant technological developments (such as digital media replacing the DVD and CD, laser printer replacing the ink-jet printer, digital photography replacing chemical film and plastics replacing metals and glass, etc.). It also studied trends in markets with an emphasis on understanding customers' desires in order to support decisions leading to competitive advantage (Herring, 1999). Competitive intelligence and market intelligence are actually complimentary: while competitive intelligence usually monitors broad perspectives of the external environment that may have an impact on corporations, market intelligence is focused on current situation in the markets (Dishman and Calof, 2008; Barnea, 2014). It is important to emphasize that usually competitive intelligence has a broader perspective, with a deeper view of the future, whereas marketing intelligence is focused more on the current status of the competition in the marketplace (Dishman and Calof, 2008).

One notable similarity between government and competitive intelligence is the ongoing attempt to make decision-makers acquire the most out of the intelligence products presented to them. There is a difficulty in monitoring frequently changes in the two areas of business and state security because it is quite difficult to assess the significance of signals and noises as they arrive and to predict the future, and thus reduce uncertainty (Rafii and Kampas, 2002).

Another similarity is that in both areas, intelligence is being proactive and strives to obtain information, which can alert on changes that occur in the external environment and their significances (Prescott, 1999). In both domains, the intelligence presented to decision-makers can be very often a catalyst for

further actions and new initiative to secure advantages (Johansson, Roos and Kirchgeorg, 2010).

Moreover, competitive intelligence and government intelligence usually deal simultaneously with both tactical and strategic areas to address different needs and requirements by intelligence consumers. However, the senior decision-makers tend to seek primarily strategic intelligence (Herring, 1990; Bernhardt, 2010). Often in competitive intelligence, they work closely with strategic planning units and marketing, while in government strategic intelligence, these units operate closely and often directly with the senior decision-makers (Søilen, 2015) aiming to influence and make their inputs recognized (Marrin, 2017).

Intelligence challenges in the business sector and government

In recent years, we have seen a growing recognition in the business field that competitive intelligence is becoming one of the core competencies required for the business decision-making process (Grant, 2005). Until the mid-1990s it was not clear that such a need for competitive intelligence existed. Old school business executives attained their positions in the business world where competitive intelligence was not established and therefore, relied on unorganized information, "gut feelings" and personal experience (Watkins and Bazerman, 2003).

For many years, competitive intelligence professionals focused mainly on the tactical aspect: the immediate actions by competitors and other players, finding out their short-term intentions and identifying changes in the business environment. In recent years, nevertheless, there has been an increasing recognition of the comparative advantage of strategic competitive intelligence (Fleisher, Wright & Allard, 2008) to identify and thus assess what was happening around, know who you are fighting with (Atsmon, 2017), and contribute to the planning and preparations for the coming years (Prescott & Miller, 2001). As Søilen points out, while the competitive intelligence and market intelligence functions are obviously important, there are occasions when the top management is not using affectively the intelligence capabilities as a result of the lack of awareness. (Søilen, 2017)

Unlike government intelligence which obtains secret information from large and unique resources, competitive intelligence is very careful to function under the law, and its value to business success gets a greater degree of recognition (Bulley, Baku and Allan, 2014). Its activity is based on gathering in leaner scope, mainly from public information (known as Open - Source Intelligence – OSINT), but it is still capable of achieving high-quality results by helping to create a valid intelligence picture of the dynamics of the external environment (Fuld, 2007). At the same time, competitive intelligence is evolving as the needs of businesses

change, the methodology and technological supporting tools of gathering and analyzing information becoming better and forcing this ongoing evolution of intelligence (McGonagle and Misner-Elias, 2016; Ming-Jer-Chen, 2017; Bulger, 2016). Thus, what really matters more than the type and quantity of the data is establishing a deep corporate culture of evidence-based decision making. According to O'Connell and Frick (2013) it also means encouraging everyone in the organization to use data more effectively.

Competitive and market intelligence were pioneers in developing significant capabilities in monitoring social media and using the insights obtained as an additional tool in the decision-making process (Fleisher et al. 2008; Laasko, 2016). Real time social media information, together with traditional market and competitive intelligence provide detailed pictures of the competitive landscape and allow a comprehensive story than neither can deliver alone. Big Data accelerates these capabilities. This formula was recently presented by the leading business consulting firm, McKinsey. In this important article (Harrysson, Metayer and Sarrazin, 2012), the authors stated that the business world had developed advanced analytical tools for obtaining vast business information extracted from social media in addition to "conventional" sources. Government intelligence also gives increased weight to OSINT, revealed as important and qualitative, that can hardly be ignored. If in the past, one could argue that national strategic intelligence was relying primarily on secret information, it is changing fast. OSINT is becoming highly significant and relevant, while we are living in an age of growing transparency (Larkin, 2016; Ballasy, 2015). In recent years, social media has become a significant source for intelligence in government (Pascovich, 2013; Wheaton and Richey, 2014), while competitive and marketing intelligence has already used it for more than ten years (Degerstedt, 2015).

With the fast development of the Internet, the information revolution and more recently, the fast growth of social media, the business world has become much more transparent than in the past. Difficulties in collecting important information have declined gradually but the main problem remains in how to deal with vast amounts of information. The utmost challenge is the development of analytical capabilities that can benefit from the information collected. A new development is of social competitive intelligence, meaning competitive intelligence is better performed in a networking organization supporting the analytical process (Degerstedt, 2015).

As previously hinted, the United States Intelligence Community (USIC) is gradually granting higher priority to the value of OSINT. Since the 'Arab Spring', we have witnessed particularly the need to understand trends, preferences and perceptions among wider audiences through OSINT. This is something that the business world is already well-experienced in as a result of research and marketing intelligence that monitor massive crowds of customers. Other Western intelligence communities including Israel (Pascovich, 2013) follow

similar direction drawing similar lessons from the 'Arab Spring'.

Moreover, in the business world, one of the most useful sources of information, mainly qualitative collection, is through employees themselves. Since many of them have their own network and contacts with parties outside their company as part of their duties, they are exposed to important information on the competitive environment that can help to achieve a competitive advantage. This requires competitive intelligence professionals to build internal networks in the shape of informal relationship with relevant employees and brief them on key intelligence topics (KITs) such as changes in the competitive landscape, new moves by competitors, new technologies and innovation initiatives that come to their attention. Note that business firms are strict on keeping their activities legal and by codes of ethics and are careful to act in this way. In recent years, with the rapid development of OSINT and particularly social media, many companies have maintained contacts with their employees by using internal social media systems and other applications to share useful competitive information timely (Mayeh, Scheepers and Valos, 2012). Senior executives and managers are longing to be in a strong competitive position actively supported by intelligence capability, as Cisco's CEO John Chambers said: "We understand the market, our competitors and - most importantly - how our competitors think… I have a pretty good idea what their next two moves will be." (Swartz, 2013).

Intelligence failures in national intelligence

In both government and business there are real anticipations that the intelligence will deliver a timely warning on threats. But there still many setbacks thus it is important to examine one of the most important issues in intelligence, intelligence failures. One of the definitions of intelligence failure is taken from the CIA (CIA, 2008) as follows: "Systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses." According to another definition, intelligence failure is "organizational surprise resulting from incorrect information, a lack of information, from neglect or inadequate hypotheses." (Johnston, 2005). Intelligence failures often involve the late detection of a significant threat that gives a substantial advantage to the initiator side resulting in significant damage to the other side (Bar-Joseph and McDermott, 2017, pp 13-17). Examining the failures and the reasons for their occurrence leads to the conclusion that in many cases, it was possible to prevent them (Pillar, 2012; Travers, 2008). The reasons for failures usually do not arise from a lack of information but rather the human factor, i.e.: a lack of understanding the meanings of available information and poor evaluation of new and unfamiliar threats (Bar-Joseph and McDermott, 2017). The result is a wrong representation of the threat's meaning, organizational failures and difficulties in the application of the 'intelligence culture' (Davis, 2004, Mouton, 2002). Too often this is also a result of the diffusion of political considerations into intelligence assessments, i.e.

Politicization of intelligence (Maoz, 2006), and could be seen in the "Report on the U.S Intelligence Community's Prewar Intelligence Assessment on Iraq", from 2004 (Travers, 2004). However, when heads of states are refraining from intelligence warning, it is not considered an intelligence failure by the intelligence organization but a policy and decision making failures (Jensen, 2012).

One of the leading Israeli scholars within the field of military and security strategy, Yehoshafat Harkabi, emphasized that the lack of threat's distinction is a result of cognitive failures causing difficulties to produce a realistic picture (Harkabi, 1971). After failures of strategic intelligence at the national level, usually governments conduct a comprehensive examination into the causes of failures to avoid them in the future, and expose their results to the public (The 9/11 Commission Report, 2004). Expectations of improving the quality of intelligence with the increase of resources and tools in recent years did not materialize, and intelligence capabilities of the American, British and Israeli intelligence did not show significant improvements while the reasons for these failures remained the same (Betts, 2002; Betts 1978).

Nevertheless, in government intelligence, information sharing is one of the most problematic issues and an important lesson learned from the Inquiry Commission into the 9/11 terrorist attack. Its implementation has difficulties and has had internal opposition due to a disproportionate amount of secrecy and compartmentalization, resulting from limited vision and fixation of thought (Treverton, 2009). In the opinion of the 9/11 Inquiry Commission, this was one of the major faults that caused the failure of the intelligence that could prevent the terrorist attacks of 9/11 (The 9/11 Commission Report, 2004). We have also seen this problem in the intelligence failure to prevent the terrorist attack in the Boston Marathon in April 2013 (Giuliano, 2014).

As a result, following the 9/11 attacks and the subsequent failure to properly assess Iraq's Weapons of Mass Destruction program in 2003, two intelligence failures exhibiting two completely different types of errors, (Betts, 2007) official investigations were conducted to determine their underlying causes. Unfortunately, no consideration was given to look at inputs from the analytical models used in the business sector. No serious consideration was given to explore outside of the box of already known analytical practices used by the business community and academia.

Intelligence Failures and Lessons Learnt from the Business Field

As previously stated, intelligence failures also occur in the business world; however, the definition is slightly different. Intelligence failure in business can be defined as a significant surprise caused by an erroneous assessment of the competitive environment (Tsitoura and Stephens, 2012). Unfortunately, a

comprehensive review processes and lessons learned from business failures are less common as corporations keep these lessons inside (Barnea, 2011). However, in recent years it has been acknowledged that some of the reasons behind business failures also lie in the lack of an appropriate intelligence process and difficulties of managers to identify changes in the business environment. This is precisely what happened to Nortel, once Canada's largest technology company and a world leader in telecommunication. In the late 1990s, Nortel senior management failed to acknowledge early-warning signals provided by its competitive intelligence unit regarding major changes in the competitive environment (Schoemaker, Day, and Snyder, 2012), which was one of the key factors led Nortel to its collapse (Calof, Mirabeau and Richards,2015). In 2009 Nortel filed for bankruptcy protection, the single biggest corporate failure in Canadian history.

Academic research in business failures does not often highlight failures of intelligence, but rather studies other causes, such as unsuitable products, inadequate pricing, slow reaction to the competition, wrong strategic moves, and personal management failures of executives (Coyene and Horn, 2009). In numerous cases, especially failures in large corporations, while the consequences of failures were high, the corporations could recover in a reasonable time and therefore, was lesser impact than similar consequences in government intelligence failures. Some of the most serious threats to companies might not even be perceived as such in time as a result of cognitive biases, which affected on avoiding the use of the intelligence reports (Stahl and Grigsby, 1992). Acceptable solutions for business failures such as replacing senior management and organizational changes do not address the lack of intelligence or deficient attention by the decision makers focusing accidentally in failures of preparation and poor performance. A compelling example is the business failure by Levi's (Olson, van Bever and Verry, 2008) and Nokia (Surowiecki, 2013), while senior executives in each of these world leaders misread the early-warning signals which they held. Around the world and also in Israel, it seems that the number of directors understanding that quality and timely intelligence is critical to business success is increasing and therefore, moves to implement the discipline of competitive and market intelligence into their organizations become common practice.

At the same time, conventional business thinking has recognized for some years now that competitive and market intelligence studies are rooted in the experience obtained from the national intelligence (Kelley, 1968) in several fields:

1. Implementation of 'the intelligence cycle' into the business intelligence process,
2. Focus the intelligence methodology in the firm around Key Intelligence Topics (KIT's),
3. Setting up closed interactions between intelligence units and decision-makers using intelligence indicators for warning of threats in the competitive environment. For example, intelligence indicators could include loss of market

share, difficulties with major customers, decreased interest in competitors by the senior management, ignoring new competitors, and lack of knowledge about competitors and trends of innovations. The challenge is to implement a new cross-organizational discipline, which often faced company-wide objections (Søilen, 2017). This challenge of building an internal culture of intelligence was the focal point in the paper by Arthur D. Little's consultancy: "The Art of Systematic Surveillance" about implementing competitive intelligence in organizations (Johansson, Roos, and Kirchgeorg, 2010).

While the U.S. intelligence community mistakenly thought that it could not learn from experience gained by business intelligence, the business world has vast and successful experience using marketing research and collecting public information to identify consumer preferences and analyze competitors' moves. The recent failure of the intelligence in predicting the events of the 'Arab Spring' was noted by deputy director of the DIA, David Shedd: "analysts failed to note signs that would have indicated to us, shown us, that there was a growing dissatisfaction ... in the general population. We missed that." (Dilanian, 2012). These events led the U.S. intelligence agencies to examine relevant business experiences, analyzing the positions of broad audiences (crowd sourcing) in conjunction with academia and many global companies, including Intel, HP, Dell, Google, Eli Lilly, Procter & Gamble and General Electric.

An additional field that allows American intelligence to learn from these business experiences is in forecasting markets (Betts, 2004), known as prediction markets. This extensive business experience allows us to estimate the directions and trends in the markets and get early warnings of possible significant changes (Yeh, 2006). Another area were intelligence communities in the US and Israel have looked recently towards is the experience acquired by the business sector in measuring performance and specifically, the value of information (Hendriks and Wooler, 2006; Hollister Hedley, 2005; Gilad and Orbach, 2012; Moore, Krizan, and Moore, 2005).

The interrelations between national intelligence and competitive intelligence. A case study[iii]

Zim Ltd. was a leading Israeli corporation in the shipping business, among the 10 largest in the global industry of marine containers. In 2009, Zim made a presentation to its bondholders, in preparation for a discussion about the possibility of deployment its debts. The presentation, showed the predicted

iii The content of this case study was previously presented in a paper published by the same author in Competitive Intelligence Magazine, Vol. 16, No. 3, July- September, 2013. This case study about Zim Ltd is based upon two sources: Sheva, 2009 and Zur, 2009. It is presented briefly, yet the aspects of the intelligence failure have been analyzed carefully, miscalculated decisions being given special consideration.

increase in the volume of maritime transport as well as the volume of investments in building new ships expected to be watered in the coming years. Because the shipbuilding industry has open access to all of its records, it was possible to see that the production rate of ships was growing faster than the projected rate of cargo. According to this presentation, the availability of marine transportation was expected to increase between 2000 to 2013 by three and a half times, from 4.9 million TEU (unit of measurement accepted in containers) by 2000 to 17.9 million TEU by 2013. There has been no increase of this magnitude in 13 years and thus there was a surplus of shipping capacity of containers. In fact, in 2008, the situation became worse due to a decrease in ship demands, which exacerbated the problem of overcapacity in shipping transport dramatically.

However, even without this decrease in the demand for shipping capacity, there was still an over capacity that resulted from building too many ships. If Zim could see the surplus capacity expected for sea transport, then why did it enter into a strategic plan of acquiring more ships and accumulate a significant debt, a plan that could compromise its very existence?

The 2004 annual report by Israel Corporation Ltd., Zim's parent company, had predicted the following based on intelligence reports: -"management of Zim ships mentioned that the supply growth rate is expected to be higher than the growth in demand for transport of containers, given the increase in new orders for ships under construction. Such growth could have a significant impact in the business of leading marine companies"-. If this situation was evident already in 2004 – too much supply of transport capacity and the same statement appeared in the management reviews, then the question remains why did Zim enter into a massive investment program in 2006 and 2007 and order new ships?

If a competitive intelligence analyst identifies expected surplus capacity in two or three years, the most logical thing to do is to advise the senior management to replace the fixed costs with variable costs and reducing debt. Meaning, it is not worth buying ships and equipment or to call long-term lease agreements - better to sell ships to shorten long-term leases and short-term contracts. In this way, when it was low season, one can easily reduce costs and return ships whose lease dates have expired. However, such tactics would hurt profitability in the short term, for a price of increasing the running costs for future flexibility and reducing risk. Second, no one wanted to be the one that contracts in a growing industry. Therefore, management tends to follow the trend of other companies. This was a familiar human weakness and also a cognitive bias: we prefer to be wrong with everyone than to be right alone. There is a lesson to be learned from this case: people working in the business world should avoid groupthink. The excess of current production capacity was a heavy burden on Zim's shoulders for four and five years since 2009, which later led it into bankruptcy.

But what are the lessons learned from the competitive intelligence aspects? Was it possible to avoid the catastrophic financial situation Zim reached in

2009 through the use of competitive intelligence analysis? The clear answer is yes. Competitive intelligence is also about identifying the big trends that will reshape the business environment and the drivers that disrupt the industry. Because various industries have available information, it is possible to forecast and predict based on reported number. This analysis will help identify which trends are of the highest impact, uncertainty and will allow scenario generation to better address and mitigate potential failures.

Intelligence tools we know from national strategic and business intelligence could have help the decision-makers at Zim. The use of Forecasting, Strengths, Weaknesses, Opportunities, Threats (SWOT) analysis and OSINT (Table 1 column 2), was not enough to have a strong impact on the decision -makers, who ignored this analysis which later brought Zim to bankruptcy. Zim could have improved its intelligence performance by using tools acquired from the national intelligence discipline (Table 1, Column 3, in bold letters), like Early-Warning indicators; in order to know better about threats as a result of global changes in the international commerce – KITs - to improve focus on what was really important for Zim to know at that stage and Opportunity Analysis - which could have helped identify external opportunities and vulnerabilities that could have been exploited to advance a much more careful strategy at that time. (Rothwell, 2012). Only concise strategic intelligence efforts could give Zim's decision-makers the inconvenient truth of what's really going to happen to Zim's if it ignores the drivers of change in the competitive arena.

Table 1: Zim Ltd.: Using intelligence tools to improve the decision- making process

Areas of activity (1)	**Imported tools from competitive intelligence (2)**	**Imported tools from national intelligence (3) (*potential*)**
Analysis	SWOT	Early warning indicators
Gathering	OSINT	Key Intelligence Topics (KITs)
Management of uncertainties	Forecasting	Opportunity analysis

Conclusions

Intelligence failures by the U.S. intelligence community as well as other intelligence organizations in the last decade, including missing the prediction of the 'Arab Spring', led U.S., UK, and Israeli intelligence agencies to examine

the accuracy of relevant experiences in business analysis of large audiences, performing forecasting, using opportunity analysis techniques and also to measure the value of information, as is well-known in the business world.

It seems that national intelligence organizations have gradually started to comprehend the need to study other disciplines, including the business field including competitive intelligence, to see how they could enhance their abilities and to open up to the business sector and implement new capabilities that after making adjustments, could help to confront the challenges they are facing. An excellent example is how the FBI reinvented itself after 9/11 and reorganizes itself from a law enforcement agency to intelligence security agency as a result of a notable study by three notable scholars from Harvard headed by Jan Rivkin, using specialized academic capabilities in organizational design and organizational identity (Gulati, Raffaelli and Rivkin, 2016).

Those engaging in competitive and market intelligence constantly strive to reach the highest professional level recognized by national intelligence and see there the true model for information and intelligence management which are supporting the decision making process by governments. On the other hand, the author's belief is that by using the intelligence discipline it was possible to create early warnings before the burst of the 2008 financial crisis (Walton, 2012, Barnea, 2011), that could give timely early warning signals that could help to prevent this crisis which changed the economic history of the world. This is also true to many other strong corporations, which failed to see the changes coming by competitors and strategic market's moves, which left them with no likelihood to survive.

In both government and in business the intelligence discipline is a decision support system. The use of an intelligence approach is an important way of assisting chief executives in both fields in avoiding mistakes in the process of deciding what to do next. It leads to a more careful evaluation of alternatives and dimensions in a comprehensive way, thus overcoming many of the problems associated with biases in information processing, biases in group dynamics and in individually decision-making. In addition, intelligence analysis has the benefit of displaying all the information in a systematic way for key decision makers.

The author's belief is that it is necessary to build new bridges between national intelligence officials and executives in the business world, to discuss the mutual benefit from learning from each other. To overcome the issue of secrecy, which characterizes national intelligence, it has to be clarify in advance, that these discussions will be focused on methodology without breaching state secrets. This is a major challenge when trying to achieve mutual learning of intelligence. As could be seen in table 1, in Israel we have identified intelligence tools that could be imported from competitive intelligence to government intelligence and vise versa, from the national intelligence to competitive intelligence. We are in the initial stage of this kind of discussion, especially after national intelligence found the necessity to open itself, but it is not an easy process.

Endnotes:

April, K., and Bessa, J. (2006). "A Critique of the Strategic Competitive Intelligence Process within a Global Energy Multinational". *Ashridge Business School UK*.

Atsmon, Y. (2017, June, 27). "To Develop a Winning Strategy, Know Who You Are Fighting", *McKinsey & Company*, retrieved from www.mckinsey.com.

Ballasy, N. (2015). "Brennan: CIA Must Rely on Social Media in the Middle East", PJ Media. Retrieved from http://pjmedia.com/blog/brennan-cia-must-rely-on-social-media-in-the-middle-east/.

Bar-Joseph, U., and McDermott, R. (2017). *Intelligence Success & Failure, The Human Factor*, Oxford University Press.

Barnea, A. (2011). "Financial Crisis as an Intelligence failure", *Competitive Intelligence Magazine*, Vol. 14, No.2, April/June.

Barnea, A. (2011). "Lack of Peripheral Vision, How Starbucks Failed in Israel?" *African Journal of Marketing Management*, Vol. 3 (4), April: 78-88.

Barnea, A. (2014). "Competitive Intelligence in the Defense Industry: A Perspective from Israel – A Case study analysis", *Journal of Intelligence Studies in Business*, Vol. 4, No 2: 91-111.

Barnea, A. (2015). "Failures in National and Business Intelligence: a Comparative Study", A Thesis Submitted for the Degree of Doctor of Philosophy, University of Haifa, School of Social Sciences.

Berenhardt, D. (2010). "Strategic Intelligence for Executives", *Wits Business School Journal*, Vol. 3, issue 22.

Betts, R. (2002). "Fixing Intelligence". *Foreign Affairs*, 81: 43–59.

Betts, R. (2004). "Analysis, War and Decision: Why Intelligence Failures Are Inevitable?", *Strategic Intelligence: Windows into a Secret World, an Anthology*, eds. Johnson, L., and Wirtz J., LA, Roxbury Publishing Co. 97-99.

Betts, R. (2014). "Analysis, War and Decision: Why intelligence failures are inevitable", *Journal of the American Intelligence Professional*, COO612718.

Betts, R. (2007). "Two faces of intelligence failure: September 11 and Iraq's missing WMD". *Political Science Quarterly*, 122(4): 585-606.

Bulger, N. (2016). "The Evolving Role of Intelligence: Migrating from Traditional Competitive Intelligence to Integrated Intelligence", *The International Journal of Intelligence, Security and Public Affairs*, 18:1: 57-84.

Bulley, C., Baku, K., and Allan, M. (2014). "Competitive Intelligence Information: A Key Business Success Factor", *Journal of Management and Sustainability*; Vol. 4, No. 2.

Busenitz, L., and Barney, J. (1997). "Differences between entrepreneurs and managers in large organizations: Biases and heuristics in strategic decision-making" *Journal of Business Venturing* Volume 12, Issue 1, January: 9-30.

Calof, J., Mirabeau, L., and Richards, G. (2015). "Towards an environmental awareness model integrating formal and informal mechanisms – Lessons learned from the Demise of Nortel", *Journal of Intelligence Studies in Business*, Vol. 5, No. 1: 57-69.

Central Intelligence Agency, (2017, June 3). "Chapter one: Definitions", *Center for the*

Study of Intelligence. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence.

Central Intelligence Agency, (2017, June 3). "INTellingence: Open Source Intelligence", *News and Information*. Retrieved from https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/open-source-intelligence.html.

Coyene, K. and Horn, J. (2009). "Predicting you Competitor's Reactions", *Harvard Business Review*, April.

Davies, P. (2004). "Intelligence culture and intelligence failure in Britain and the United States", *Cambridge Review of International Affairs,* Volume 17, Number 3, October 2004: 495-520.

Degerstedt, L. (2015). "Social competitive intelligence: socio-technical themes and values for the networking organization", *Journal of Intelligence Studies in Business,* Vol. 5, No. 3: 5-34.

Dilanian, K. (2012, July 19). "U.S. intelligence official acknowledges missed Arab Spring signs", *Los Angeles Times*. Retrieved from http://latimesblogs.latimes.com/world_now/2012/07/us-intelligence-official-acknowledges-missed-signs-ahead-of-arab-spring-.html.

Dishman, P., and Calof, J. (2008). "Competitive intelligence: a multiphasic precedent to market strategy", *European Journal of Marketing*, Vol. 42, No. 7/8: 766-786.

Fleisher, C., Wright, S., and Allard, H. (2008). "The Role of Insight Teams in Integrating Diverse Marketing Information Management Techniques". *European Journal of Marketing*, Vol. 42, No. 7/8.

Fuld, L. (2007). *The Secret Language of Competitive Intelligence,* Crown Business.

Gilad, A. and Orbach, M. (2012, July 1). "8200 Silicon Valley Corner: The IDF's largest unit is learning to work like a start-up", *Calcalist*. Retrieved from (Hebrew) http://www.calcalist.co.il/internet/articles/0,7340,L-3575727,00.html.

Gilad, B. (2004). *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk and Create Powerful Strategies*. New York, NY, Amacom.

Giuliano, M. (2014). "How the FBI Is Evolving to Meet Threats in a Changing Environment", *From the Boston Marathon to the Islamic State, Stein Counterterrorism Lectures,* Maththew Levit (ed.), The Washington Institute for Near East Policy, Vol. 6: 9-16.

Grabo, C. (2004). *Anticipating Surprise: Analysis for Strategic Warning.* University

Grant, R. (2005). *Contemporary Strategy Analysis*, Blackwell Publishing.

Gulati, R., Raffaeli, R., and Rivkin, J. (2016). "Does 'What We Do' Make Us 'Who We Are'? Organizational Design and Identity Change at the Federal Bureau of Investigation", *Harvard Business School*, Working Paper 16-084, January. 12.

Harkabi, Y. (1971). *Fundamentals in the Israeli Arab Conflict*, Ministry of Defence publishing, Tel Aviv, Israel (Hebrew).

Harrysson, M., Metayer, E., and Sarrazin, H. (2012). "How 'Social Intelligence' Can Guide Decisions", *McKinsey Quarterly*, November.

Hendriks, B., and Wooler, I. (2006). "Establishing the return on investment for information and knowledge services: A practical approach to show added value for information and knowledge centres, corporate libraries and documentation centres", *Business Information Review*, V. 23(1: 13-25.

Herring J. (1990). "Senior Management Must Champion Business Intelligence Program", *Journal of Business Strategy,* September-October, pp 48-52.

Herring, J. (1999). "Key Intelligence Topics: A Process to Identify and Define Intelligence Needs", *Competitive Intelligence Review*, Vol. 10(2): 4–14.

Hollister Hedley, J. (2005). "Learning from Intelligence Failures", *International Journal of Intelligence and CounterIntelligence, Vol. 18, No. 3, fall*: 435–450.

Jaworski, B., Macinnis, D., and Kohli, A, (2002). "Generating Competitive Intelligence in Organizations", *Journal of Market-Focused Management*, 5: 279– 307.

Jensen, M. (2012). "Intelligence Failures: What Are They Really and What Do We Do about Them?", *Intelligence and National Security*, Vol. 27, Issue 2: 261-282.

Johansson, A., Roos, D., and Kirchgeorg, V. (2010). "The Art of Systematic Surveillance", *Arthur, D. Little.*

Johnston, J., and Johnston, R. (2007). "Testing the Intelligence Cycle Through Systems Modeling and Simulation", *Center of the Study of Intelligence, Central Intelligence Agency.* Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence.

Johnston, R. (2005). "Analytic Culture in the US Intelligence Community: An Ethnographic Study". *Center for the Study of Intelligence, Central Intelligence Agency.* Washington, DC, 20505.

Kahneman, D., and Tversky. A. (1984). "Choices, Values, and Frames", *American Psychologist,* 39: 341-350.

Kelley, W. T. (1968*). Marketing Intelligence: The Management of Marketing Information,* London: Staples Press.

Laakso, T. (2016). "Handbook of Social Media Intelligence", *M-Brain*, www.m-brain.com

Larkin, S. (2016). "The Age of Transparency", *Foreign Affairs*, May/June, vol. 95, no. 3: 136-146.

Maoz, Z**.** (2006, August 31). "Intelligence Failures: An Analytical Framework", *Paper presented at the annual meeting of the American Political Science Association,* Marriott, Loews Philadelphia, and the Pennsylvania Convention Center, Philadelphia, PA.

Retrieved from http://www.allacademic.com/meta/p151465_index.html.

Marrin, S. (2017). "Why strategic intelligence analysis has limited influence on American foreign policy", *Intelligence and National Security.* Retrieved from http://dx.doi.org/10.1080/02684527.2016.1275139.

Mayeh, M., Scheepers, R. and Valos, M. (2012). "Understanding the Role of Social Media Monitoring in Generating External Intelligence*", 23rd Australasian Conference on Information Systems,* 3-5 Dec, Geelong.

McGonagle, J., and Misner-Elias, M. (2016). "The Changing Landscape of Competitive Intelligence: Two Critical Issues Investigated", *Salus Journal*, Issue 4, Number 1.

Ming-Jer-Chen, (2017). "Competitor Acumen, the Heart of Competitor Analysis", Darden *Business Publishing, University of Virginia*, UVA-S-0293, April 10.

Miscik, J. (2017). "Intelligence and the Presidency, How to Get it Right", *Foreign Affairs*, May/June.

Moore, D., Krizan, L., and Moore, E. (2005). "Evaluating Intelligence: A Competency-Based Model", *International Journal of Intelligence and CounterIntelligence*, Vol. 18, No. 2, summer: 204–220.

Mouton, T. (2002). "Organizational Culture's Contributions to Security Failures". Retrieved from www.zoklet.net/totse/en/politics/central.../167571.html.

Myers, C. (2015). "Is Your Company Encouraging Employees to Share What They Know?", *Harvard Business Review*, Nov. 6.

O'Connell, A. and Frick, W. "You have got the information, but what does it mean? Welcome to from Data to action", *Harvard Business Publishing*, (2014). Retrieved from https://hbr.org/2013/11/youve-got-the-information-but-what-does-it-mean-welcome-to-from-data-to-action.

Olson, M., van Bever, D., and Verry, S. (2008). "When Growth Stalls", *Harvard Business Review*, March 2008.

Omand, D. (2010), *Securing the State*, C Hurst & Co Publishers Ltd : 113-137.

Pascovich, E. (2013). "Intelligence Assessment Regarding Social Developments: The Israeli Experience", *International Journal of Intelligence and CounterIntelligence*, 26, 1: 84-114.

Pillar, P. (2012). "Presidents Make Decisions Based on Intelligence", *Foreign Policy*, Jan/Feb.

Porter, M. (1980). *Competitive Strategy: Techniques for Analyzing Industries and Competitors,* The Free Press, NY.

Prescott, J. (1999). "The Evolution of Competitive Intelligence, Designing a Process for Action", *APMP*, Spring.

Prescott, J., and Miller, S. (2001). *Proven Strategies in Competitive Intelligence: Lessons From the Trenches,* Willey & Sons, New York, Press of America.

Rafii, F. and Kampas, P. (2002). "How to Identify Your Enemies Before They Will Destroy You", *Harvard Business Review*, Nov.

Rothwell, K. (2012). "Opportunity Analysis in an Intelligence Context", *Competitive Intelligence Magazine*, Vol. 15, No. 1 January/March.

Sage, Andrew P. (1990). "Human Judgment and Decision Rules", *Concise Encyclopedia of Information Processing in Systems and Organizations*, ed. Andrew P. Sage. New York, NY: Pergamon Press, : 227-229.

Schoemaker, P. Day, G. and Snyder, S. (2012). "Integrating organizational networks, weak signals, strategic radars and scenario planning", *Technological Forecasting & Social Change*, 80, 815–824.

Sheva, N. (2009. August 27), "Zim lost 186 million $", *The Marker* (Israel, Hebrew edition). Retrieved from http://www.themarker.com/tmc/article.jhtml?ElementId=nl20090827_78683.

Smith, T. (2003). Encyclopedia of Central Intelligence Agency, Infobase Publishing: 137-138.

Søilen, K.S. (2015). "A place for intelligence studies as a scientific discipline", *Journal of Intelligence Studies in Business*. Vol. 5, No 3: 35-46.

Stahl, M., & Grigsby, D., (1992), *Strategic Management for Decision Making*, New York, NY: KWS Kent Publishing.

Steele, D. R.. (2008). "The Open Source Program: Missing in Action", *International Journal of Intelligence and CounterIntelligence,* Vol. 21. No. 3 :609-619.

Surowiecki, J. (2013). "Where Nokia Went Wrong?", *The New Yorker*, September 13,

Swartz, J. (2013). "Cisco's Chambers: 2 days with man on a mission at CES", *USA Today*, Jan. 9. Retrieved from http://www.usatoday.com/story/tech/2013/01/09/cisco-ibm-oracle-

hp/1791255/

"The 9/11 Commission Report", (2004): 435-450, Retrieved from http://www.9-11commission.gov/report/911Report.pdf.

Tianjiao, Qui. (2008). "Scanning for competitive Intelligence: the managerial perspective", *European Journal of Marketing*, Vol. 42, No. 7/8: 814-835.

Travers, R. (2004). "Report on the U.S Intelligence Community's Prewar Intelligence Assessment on Iraq". Retrieved from http://web.mit.edu/simsong/www/iraqreport2-textunder.pdf

Travers, R. (2008). "The Coming Intelligence Failure, A Blueprint For Survival", *CIA, Center for the Study of Intelligence*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/97unclass/failure.html

Treverton, G. (2009). *Intelligence for an Age of Terror*, NY, Cambridge University Press: 1-14.

Tsitoura, N. & Stephens, D. (2012). "Development and evaluation of a framework to explain causes of competitive intelligence failures", *Information Research*, 17(2) paper 521.

Vedder, R. G. & Guynes, C. S. (2000). "A study of competitive intelligence practices in organizations", *The Journal of Computer Information Systems*, 41(2): 36-39.

Walle, A. (2001). *Qualitative Research in Intelligence Marketing; the New Strategic Convergence.* Westport, Connecticut: Quorum Books.

Walton, T. (2012). "*The 2007-20098 Financial Crisis as a Way to Better Understand Intelligence Failure"*, presented in ISA conference, April. Retrieved from http://isanet.ccit.arizona.edu/MyISA/Validated/ConferenceParticipation.aspx?ConferenceID=25&View=MyProgram.

Watkins, D., and Bazerman, M. (2003). "Predictable Surprises: The Disaster you should have seen Coming", *HBR OnPoint*, # 337X.

Welch, J. (2005). *Winning*, NY, HarpersBusiness.

Wheaton, K. and Richey, M. (2014), "The Potential of Social Networks in Intelligence", *E-International Relations*, January.

Wright, S. and Calof, J.L. (2006), "The quest for competitive, business and marketing intelligence: a country comparison of current practices", *European Journal of Marketing*, Vol. 40 No. 5/6: 453-65.

Yeh**,** P. (2006). "Using Prediction Markets to Enhance US Intelligence Capabilities", *Studies in Intelligence* , Vol. 50, No. 4.

Zur, D. (2009, August, 23). "They sail with the herd", *The Marker* (Israel, Hebrew Edition). Retrieved from http://www.themarker.com/tmc/article.jhtml?ElementId=nl20090827_78683.

Reflection Paper

French Intelligence Analysis

Olivier Chopin[i]
Benjamin Oudet[ii]

Compared with Intelligence Studies from the Anglosphere, Intelligence Studies in France are experiencing a later development. It was not until the late 1990s that the first academic research programs in History were formed: most of the works focused on the progressive constitution of intelligence bureaucracies during the 19th century, up to the Second World War[I]. Despite the publication of significant academic research and the growing interest in the subject, we can argue that French Intelligence Studies remain in a state of infancy: no academic journal is specifically devoted to it in France, and there is no research centre within which it would be a specific topic, alongside International Relations and Strategic Studies. University courses and diplomas exclusively dedicated to the profession of intelligence analysis are extremely rare. It is one of the paradoxes of the French situation: the academic study of intelligence took a long time to structure itself, while France is one of the few European countries to rely on many intelligence services (internal and foreign services), for political and military decision-making, and with cutting-edge technical and human collection capabilities. Moreover, intelligence is at the heart of the state's sovereignty, in foreign policy and in support of military interventions. Foreign intelligence is both a vector of influence and a central tool for the ambition of French strategic autonomy. The French doctrines officially acknowledge the function of "knowledge and anticipation" as the first strategic function - with deterrence, protection, prevention and intervention - and the basis of the French State external action in the field of defence and security.

Like other Western intelligence systems, the French community, formally established in 2014, has as its primary function the production of analysis for political and military decision-makers. The French community includes six

i Sciences Po, Paris, France. Email : olivier.chopin@gmail.com,

ii University of Poitiers, France. Email : benjamin.oudet@univ-poitiers.fr .

main services: three of them operate under the authority of the Ministry of the Armed Forces (DGSE, DRM, DRSD), one under the Ministry the authority of the Interior (DGSI) and two under the authority of the Ministry of Finance (DNRED and TRACFIN)[2]. What is remarkable about the French intelligence community is its very late emergence (from the 2008 White Paper on Security and Defence) and the process of centralization and institutionalization of intelligence it involved[3]. That means a cultural revolution within the security and defence apparatus.

Yet, relations between universities and the intelligence services are not natural in France. On the one hand, it comes from the philosophical and theoretical genesis of the French State. The action of the French State is based on the belief that the knowledge necessary for its action is specific to the State and is of a different nature from the knowledge produced by universities[4]. Therefore, from the State's standpoint, there is no need to integrate academic knowledge and methods during the analysis phase. Indeed, traditionally, intelligence is not in French doctrine understood as a "certain kind of knowledge" and bridging the gaps with academic methods is far from obvious[5]. On the other hand, this is due to a sociological factor marking a clear dividing line between senior officials and academics, who would not belong to the "same intellectual world" and would be two "tribes" impossible to mix. This line drawn between insiders and outsiders is very clear. It is worth noting that until recently, academics in France did not recognize intelligence as a topic important and legitimate enough to be studied by the French social sciences. This naturally delayed the emergence of an interdisciplinary field of research that could mimic the Anglo-American Intelligence studies. Intelligence (*renseignement*) was associated with a remanence of the reason of State (*raison d'Etat*), a monarchical and harmful idea, doomed to disappear by the extension of the rule of Law[6].

The particular phase of analysis within the intelligence cycle is not yet the subject of specific work aimed at creating bridges between academic research and practitioners. This is one of the defining feature French analysis: Academic knowledge is not central to it and is not yet a natural component of intelligence analysis. This fact can be explained first by the recruitment methods of analysts in France. They are recruited by public administrations after competitive examination: category A (degree), category B (from the baccalaureate) and C (no diploma). Thus, training by the University is at best done in the first cycle, before individuals enter a service. Intelligence training is conducted internally, within the service. Over the past fifteen years we observe that recruitment is based on higher diplomas standards. And the trend is to recruit more qualified individuals who graduated at the master degree level.

In addition, an Intelligence Academy was created in 2010 and has the mission to develop of a common culture between services through common education and training. These courses are partly taught by academics hired for this purpose.

The Academy is not a place of recruitment but is better understood as a pool where new recruits follow common courses in order to create links between the services to which they belong. Since 2008, the creation of the Intelligence Community was a structural response to the overly vertical functioning of the intelligence services whose production of analysis was by vocation to their Minister's Cabinet. Analytic production flowed vertically to each Minister but did not beneficiate to other intelligence services. This indicated the absence of a French national intelligence cycle: each service developed an internal intelligence cycle independently of other services and for "his" consumer. Over the past ten years, two entities have been created to address that issue: The National Intelligence Coordinator in 2008 and the Intelligence Academy in 2010. Both aim at breaking the tyranny of stovepipes, described in the American context by Gregory Treverton, and at promoting the emergence of a true "community" through common training[7].

Intelligence services do not have a monopoly of analytical production for political and military decision-makers in France. Relations between the State and universities take place mainly in institutions such as the IRSEM (Institute for Strategic Research), DGRIS (General Directorate of International Relations and Strategy) and INHESJ (National Institute for Security Studies and Justice) which do not belong to the French intelligence community. The role of academic research and academics is evolving[8] and rather lies in those institutions, which take part in high-level specialized training in the State civil service and provide additional training in highly specialized areas or be recruited as contractors for a limited period of time within intelligence services.

Endnotes:

*01_* Olivier Forcade, 'Objets, approches et problématiques d'une histoire française du renseignement : un champ historiographique en construction', *Histoire, économie & société* 31e année, no. 2 (8 August 2012): 99–110; Jean-Claude Cousseran and Philippe Hayez, *Leçon sur le renseignement* (Odile Jacob, 2017); Jean-Claude Cousseran and Philippe Hayez, *Renseigner les démocratie, renseigner en démocratie* (Éditions Odile Jacob, 2015); Sébastien-Yves Laurent et al., *Transformations et réformes de la sécurité et du renseignement en Europe* (Pessac: Presses Universitaires de Bordeaux, 2016).

*02_* 'L'académie Du Renseignement', L'académie du renseignement, accessed 20 November 2017, http://www.academie-renseignement.gouv.fr/.

*03_* Commission du Livre blanc, *Livre blanc de la défense et de la sécurité nationale*, Broché (Paris: JACOB ODILE, 2008); François Hollande, Présidence de la République, and Commission du livre blanc sur la défense et la sécurité nationale, *Livre blanc sur la Défense et sécurité nationale 2013* (Paris: DOCUMENTATION FRANCAISE, 2013).

*04_* Olivier Chopin and Benjamin Oudet, *Renseignement et sécurit*é (Armand Colin, 2016).

*05_* Olivier Chopin, 'Intelligence Reform and the Transformation of the State: The End of a French Exception', *Journal of Strategic Studies* 40, no. 4 (7 June 2017): 532–53.

*06_* Chopin.

*07_* Gregory F. Treverton, *Intelligence for an Age of Terror.*, Reprint (Cambridge ; New York: Cambridge University Press, 2011).

*08_* Benoît Durieux, Frédéric Ramel, and Jean-Baptiste Jeangène Vilmer, *Dictionnaire de la guerre et de la paix* (Paris: Presses Universitaires de France - PUF, 2017).

Reflection Paper

Terrorist Intelligence Tradecraft: - What the IC Should Know -

Ammar El Benni[i]

"Warring will be less and less confined to the battlefield, and more aimed at disrupting societies using weapons from afar or suicide terrorists from within".

(Global Trends. Paradox of Progress, National Intelligence Council, 2017)

Policy-makers are not only consumers of strategic information, but also artisans of intelligence systems meant to support national security needs. Building intelligence capabilities to fight threats of their time has always concerned decision-makers. Policymakers' support to the intelligence tradecraft has translated into policies aimed at strengthening the organization and resources of the Intelligence Community (IC); to this end, intelligence practitioners have tried to respond to the policymakers' support with a continuous improvement and adaptability of working methods for intelligence collection and analysis. In other words, while policymakers are in charge of creating an adequate institutional infrastructure for the needs of the IC, the IC must know what to ask for. This progression requires intelligence professionals to understand tomorrow's threats and therefore be able to produce actionable intelligence in the context of the Future. One of the requisites for the IC in the current Long War on Terror is the understanding of the terrorist intelligence building process. This *Reflection Paper* herein contemplates the emerging phenomenon of 'terrorist intelligence building' in the broader context of terrorists developing their own

i "Mihai Viteazul" National intelligence Academy, Romania

ability to collect, analyze and use intelligence in the planning stages of their attacks. More specifically, the paper aims at launching a discussion about the importance of understanding the information tradecraft conducted by terrorists (organizations or individuals), by considering the preparation and conducting of attacks an excellent example for this purpose, and explore what IC analysts can learn from that.

Terrorist groups have evolved within the last two decades into complex organizations having their own structures, cultures, networking system, and web of information sources. At the same time, in addition to their own ability to develop such capabilities, many of them have benefited from logistical and operational support from sponsoring entities[1]. All these elements have allowed terrorists to develop their own system of collecting and processing intelligence that is further used in planning their tactics to conduct attacks. As showcased in the Operations Security Intelligence Threat Handbook, "a group's objectives and organizational capabilities dictate which tactics it uses",[2] however, goal achievement depends on the terrorist organization's ability to receive adequate information for planning and executing an operation.

Terrorist organizations plan their attacks in advance by employing experts that identify action patterns in the preparation of such events through intelligence gathering and surveillance. For terrorist networks, the main goal of this process is to reduce operational uncertainty and to increase the impact and accuracy of the strike. Research has shown that despite prior beliefs that terrorist attacks were the result of absolute irrationality and crazy extremism, whatever the type of terrorist incident (bombings, kidnappings and hostage taking, armed attacks and assassinations, firebombings, hijackings, chemical terrorist attacks, or cyberterrorism), the tactics of terrorism are rather an instrumental approach used by rational actors to send a political message[3].

Terrorist groups use similar intelligence tradecraft techniques used by states to collect open-source intelligence and also to carry out clandestine operations[4]. Detailed and well-calculated operational intelligence represents the same valuable input to the decision-making process in terrorist organizations as well-processed intelligence does to the policy-making process aimed to combat terrorism in organized states.[ii] According to the "Declaration of Jihad Against the country's Tyrants", intelligence is defined as "...the covert search for and examination of the enemy's news and information for the purpose of using them when a plan is devised[5]"; in other words, as the *Encyclopedia of Afghan Jihad* states, "[i]ntelligence is providing the necessary information for policy-making[6]". The policy-making process in government parallels with a complex series of actions consisting in both tactical operations and strategic planning aimed to support the Terrorist Attack Cycle[7] in terrorist organizations. Thus,

ii In this paper, the term decision-making will be applied to the use of intelligence by terrorists and policy-making to the use of intelligence by organized states.

knowledge developed by terrorists serves various tactical and strategic functions such as: the exploitation of enemy vulnerabilities (which contributes to the selection of targets, but also to the 'decredibilization' of the enemy-target within the terrorist organization), the understanding of the target's culture, resources and methods (to decide on the best method of attack)[8] or the recruitment of new insiders[9] (identify groups and individuals that might join the terrorist cause).

Terrorist intelligence can be both openly-available and covertly-obtained information generated through research on a target, or the result of collection engaged through covert means – such as the use of insiders within a target. Similar to the traditional Intelligence Cycle used by governments, the collection and analysis of information take place in the first two [out of seven phases] in the Terrorist Attack Cycle;[iii] these phases consist of (i) target selection, and (ii) attack planning. Intelligence gathering and surveillance, together with operational analysis, are an integrated process during which the two phases succeed each other until the optimal decision regarding the chosen target and the attack strategy is established. The gathering or collection of Intelligence moves from general to specific information, and the research process begins with the mapping potential targets (that could match the desired outcome requirements) and continuing with the identification of those particular details that might help in the achievement of the highest impact. The analytic process is permanently attached to information gathering and consists of the rational cost-benefit analysis of all the parameters that can lead to increased effectiveness of the target selection and implementation of strikes (after the information is gathered, terrorists conduct pre-operational surveillance of targets to determine which are the best ways to conduct the attack).

The intelligence collection-analysis joint process characteristic of Islamist Terrorism[iv] takes place mainly in an online environment, with Internet as the main channel and source for generating relevant intelligence for terrorists. In a 2012 Report of the United Nations Office on Drugs and Crime, various purposes of the use of the Internet by terrorist were identified[10]: 1) dissemination of propaganda (aimed at enabling recruitment, incitement and radicalization); 2) financing (through direct solicitation, e-commerce, exploitation of online payment tools, and charitable organizations); 3) training; 4) planning; 5) execution; 6) cyberattacks. Thus, rather than attacking the internet – cyberterrorism by Islamist groups being still a reduced phenomenon -, terrorists use the online environment to get free, fast and broad access to information on their potential targets and their characteristics that can be converted into vulnerabilities and

iii The steps in the Terrorist Attack Cycle have been identified as: (1) Broad Target Selection, (2) Intelligence and Surveillance; (3) Specific Target Selection; (4) Pre-Attack Surveillance and Planning; (5) Attack Rehearsal; (6) Actions on Objective; (7) Escape and Evasion.

iv This paper doesn't look at other groups considered as representative of terrorism such as the FARC or IRA.

therefore used as facilitators in the achievement of the plan:

> "Intelligence during the planning phase, therefore, sought to identify vulnerabilities that would facilitate the preferred method of attack. Although the planned use of hijacked aircraft also influenced target selection by identifying vulnerabilities consistent with the method of attack (e.g., the need for buildings to be clearly visible from the air), it was during the planning phase of the operation that intelligence made its most significant contribution. Intelligence would be used to determine those details of the plan capable of facilitating the preferred method of attack in such a way as to maximize the likelihood of success".[11]

Thus, intelligence becomes a key prerequisite and a tool meant to enhance operational certainty and increase planning effectiveness of terrorist organizations. Open-Source Intelligence for terrorist purposes can be gathered and compiled from a variety of overt materials, the majority of which are widely available online, such as books and articles, blog and web content, unclassified and declassified materials, movies, and even specialised software (such as flight simulation software used by the 9/11 terrorists for training purposes).

Although the Terrorist Attack Cycle does not explicitly include a dissemination stage aimed at providing the decision-maker of the organisation with operational intelligence, information distribution is nevertheless present throughout the entire cycle, especially in the pre-attack planning, not as a traditional briefing process of a few, but rather an instructions-giving and capabilities-building operation. Terrorist groups act as learning organizations[12] whose decentralized and networked structures enable information sharing among members, both current and future. Thus, in the context of the terrorist tradecraft, intelligence collection and dissemination achieve a more complex use. In addition to selecting their targets and selecting the best methods and technologies to design their attacks, terrorist organizations also work to identify and appoint the best perpetrators. Whether used to distribute materials anonymously or transmit a call for action, intelligence dissemination is mainly shaped as a recruitment process that is omnipresent throughout the Terrorist Planning Cycle.

The IC should make every effort to not only explain what a terrorist group is capable of doing today, but also try to predict what it might be capable of doing tomorrow. Directing analytical attention to how *terrorists achieve operational knowledge and build their human capital as part of a complex intelligence tradecraft* may provide a valuable and efficient route to gain a new edge in degrading their capabilities and reducing the effectiveness of their attacks.

Endnotes:

*01_* Operations Security. Intelligence Threat Handbook. The Interagency OPSEC Support Staff, 1996. Retrieved from https://fas.org/irp/nsa/ioss/threat96/index.html .

*02_* Ibid.

*03_* PeterR. Neumann, Michael Lawrence Rowan Smith, *The Strategy of Terrorism: How it Works, and why it Fails*. Routledge, 2008, p. 5.

*04_* Georgios Tsichritzis, *Intelligence Collection, Analysis and Reporting of Terrorist Groups: a Study of Effectiveness*. Research Institute for European and American Studies, 2015. Retrieved from www.rieas.gr.

*05_* Al Qaeda's Operational Intelligence—A Key Prerequisite to Action, Studies in Conflict & Terrorism 31:1072–1102, 2008. p.1073. *op cit.* Georgios Tsichritzis.

*06_* Ibid.

*07_* "Defining the Terrorist Attack Cycle," Stratfor, 2012. Retrieved from https://worldview.stratfor.com/article/defining-terrorist-attack-cycle. George Habash, "Terrorist Planning Cycle", Appendix A, *A Military Guide to terrorism in the Twenty-First Century*, 2007.

*08_* *Op. cit.* Georgios Tsichritzis

*09_* I. Lachow, C. Richardson, "Terrorist Use of the Internet. The Real Story". *Joint Force Quarterly.* Issue 45, 2nd Quarter, 2007.

*10_* *The Use of the Internet for terrorist purposes*, United Nations Office on Drugs and Crime, UN, New York, 2012.

*11_* Gaetano Joe Ilardi, "The 9/11 Attacks—A Study of Al Qaeda's Use of Intelligence and Counterintelligence". *Studies in Conflict & Terrorism*, 32:171–187, 2009.

*12_* Brian A. Jackson, Organizational Learning and Terrorist Groups. RAND, 2004, p.2.

Through the Cloak and Dagger Crystal Ball: Emerging Changes that will Drive Intelligence Analysis in the Next Decade

Efren R. Torres-Bacheș, Daniela Bacheș-Torres (coord.)[i]

"If you are depressed you are living in the past.
If you are anxious you are living in the future.
If you are at peace you are living in the present."

(Lao Tzu)

As part of this project aimed at providing the intelligence literature with a multi-sector comprehensive view that moves away from the mainstream government approach, we decided to ask various experts from the academic, public and private sectors to share their thoughts about the transformation of the intelligence analytic process within the next decade. The respondents were asked to provide 200-300-word answers to the following question: ***Is Intelligence analysis going to be any different in 10 years from now?***

With the emergence of new threats and the ongoing dire re-shaping of diplomacy worldwide, it is vital that we, as scholars, experts and practitioners, ask ourselves in what direction is the intelligence practice heading towards. It is important to explore this quasi-futurist question due to the fast development of new technology for collection and analysis, as well as the increasing role and relevance of OSINT in intelligence practices. Furthermore, intelligence analysis as a profession is

i We thank all the contributors who shared their knowledge, experience, and time in this original article meant to be a first step initiative in the setting-up of a future dialogue between experts from different fields that conduct, work with, and write about intelligence analysis.

rapidly evolving and branching out to a new domain: private companies.

The application of traditional intelligence to the private sector for companies such as Disney, Netflix and Sony is a living proof that intelligence analysis is evolving to adapt to a new setting; along with this new role of intelligence in the private sector comes a new breed of intelligence analysts that have OSINT and Social Media Intelligence (SOCMINT) as their second language and are rapidly changing, through innovation, the way that intelligence analysis is being done. Thus, it is very important to ask ourselves where intelligence analysis will be in ten years. How will threats change and what capabilities will be available for analysts to use? It is the responsibility of all parties involved to discuss how intelligence, as a practice and topic of study, will evolve and adapt within the next decade to address and mitigate new and old existential threats around the world.

Future security context:

Richard Jackson *is Professor of Peace Studies and the Director of the National Centre for Peace and Conflict Studies, the University of Otago, New Zealand. He is the author or editor of ten books and more than a hundred papers on critical terrorism studies, pacifism, international conflict resolution, the causes of political violence, and political development, among others. He is also the editor-in-chief of the journal, Critical Studies on Terrorism. His most recent book is The Routledge Handbook of Critical Terrorism Studies (Routledge, 2016):*

In the coming decades, security issues will remain somewhat contested between elite and popular concerns, with the elites most likely focusing on current security issues like terrorism, cyber-security, the potential for great power war, regional flash-points, and mass immigration. Popular concerns will more likely move towards issues related to the effects of climate change, the effects of rising inequality, and the responsiveness of the political system to calls for radical overhaul. This divergence of what security entails is due to both the position of elites relative to the effects of climate change (their wealth protects them from the worst effects of climate change), and their dominant intellectual framework which remains state-centric and rooted in traditional notions of military-based superiority. For ordinary people, the effects of climate change and rising inequality, combined with the spreading knowledge of how to undertake mass nonviolent resistance, will shift their perceptions to more immediate and everyday security concerns related to quality of life.

A key unknown factor here is the role of future technological developments. Some new technologies will assist individuals and groups who want to cause violence in pursuit of their political contestation strategies, while other technologies will support the mobilisation of mass movements for change. Still other technological developments will assist governments in controlling the

masses and/or thwarting small groups of radicals. It's impossible to predict at that stage exactly which technological developments will emerge and what their impact on security will be.

However, we can be sure that the security environment is headed for a period of great instability as the effects of climate change force large-scale population movements, either through rising sea levels, the loss of life-supporting land, or the failure of poorer societies to adapt to severe changes in the climate. These population movements will in turn cause great political instability and potential social conflict, which will be the cause of many types of insecurity. The global availability of light weapons will add urgency to conflict prevention efforts. Added to this, the effects of climate change will enhance the visible effects of rising inequality and its accompanying instability. As the world's population sees the super-rich evade the effects of climate change and inequality while continuing to accumulate vast untaxed wealth, this will also cause social unrest and calls for radical, perhaps even revolutionary, reforms. If we combine this with the current rise in nonviolent mass movements around the world, the growing number of young people supporting radical politicians (Bernie Saunders, Jeremy Corbyn, Podemos, etc), and the rise of populist, often racist political movements, this provides a situation of conflict, turmoil and instability that governments may struggle to control.

Into this tumultuous situation, the temptation of governments will be to try and exert greater control over their citizens, through both covert and overt forms of surveillance, coercion and physical management. We have seen efforts to this effect already, and as demands for radical political change in order to deal with climate change and inequality grow louder, it will become more and more tempting for governments to try and crack down on what they perceive as social unrest and efforts to disturb the status quo. From this perspective, I can foresee future security threats emanating from the state itself as it tries more and more desperately to control the situation and head off challenges to its authority and the existing social order. The greatest security challenge in the coming years therefore, will be to protect people from the hundreds of thousands of excess deaths which will be caused by climate change, as well as the millions of excess deaths caused by global inequality, all while managing the popular demands which will come from civil society for a radical overhaul of the current political and economic system.

Ordinary people all over the world are waking up to the realisation that their everyday security is threatened far more by climate change and inequality than it is by issues like terrorism, cyber-attacks or possible great power war, and they want radical social and political change to meet this challenge. The question is: are political elites and security managers equipped, intellectually and materially, to meet these security challenges while also overseeing a period of potential revolutionary change in the political and social order?

Intelligence Analysis through the Experts' Lenses

Intelligence analysis in the next decade is likely to remain the same at its very core as it is a process inherently human that is only assisted by new tools and techniques. What will be changing, however, are the tools that intelligence analysts use to collect and assess information. Across all responses, three general themes were identified that will change intelligence analysis: 1) the development of new analytic tools mainly based on Artificial Intelligence (AI), 2) the increasing relevance of Open-Source Intelligence (OSINT), and 3) the issues of source validity in a world where good and distorted/manipulated information is widely accessible. The diversification of threats and the availability of new technology for these actors to use will pose a big challenge to intelligence analysis.

George Friedman *is Founder and Chairman of Geopolitical Futures (www.geopoliticalfutures.com), a publication dedicated to explaining and predicting the course of the international system. Friedman is an internationally recognized geopolitical forecaster and New York Times best-selling author. Some of his best-known books include The Next 100 Years, The Next Decade and the most recent Flashpoints: The Emerging Crisis in Europe:*

There have been two major events in intelligence over the past ten years. Both are related to digitalization of data. The first is the growing unreliability of the open source. The second is the decline in the security of classified information. Both are forcing a reverse in the process of increased reliance on non-traditional forms of intelligence.

The traditional definition of open source intelligence was material that had passed through a rigorous publishing process. The reporter gathered information whose value was judged by several layers of editors, who were, in turn, under the control of a publisher. This process provided a rigor that tended to discard poorly sourced information. As a result, what was published had a relatively high degree of reliability, and extended the reach of an intelligence organization seeking situational awareness in an effective way. Particularly with the development of the Internet, access to this information had substantial and, many experts said, growing value.

That value is in decline because of two processes. First the economic pressures of publishing have caused a deterioration in the gathering and vetting process. Second the development of a culture of crowd-sourced information (twitter, etc.) has created pressures on publications to shift to more responsive modes, thus re-broadcasting erroneous information. Attempts to use crowd-sourced information by intelligence organizations have not met with great success as the noise to signal ratio is daunting. The ability to publish without process online has closed off the open source except for the most disciplined and skillful operators.

The same process of digitalization has posed a massive security risk for

intelligence organizations. Data storage systems that are linked to the Internet are highly vulnerable. Worse, it is difficult to know if a hostile service has compromised the system. Taking storage systems offline will protect them from all but internal attack, but at a high price in efficiency for transmitting and distributing intelligence.

Both of these problems can be mitigated by skillful management. The digital world will remain. However, this now creates a pressure to reverse direction back toward more traditional modes of gathering, while using current systems as a means for shaping perceptions of other organizations and accessing vulnerable information.

Stephen Marrin *is an associate professor at James Madison University, where he is Director of the 250 student Intelligence Analysis program in the Department of Integrated Science and Technology. Holder of a BA from Colgate University and MA and Ph.D. degrees from the University of Virginia, he chairs the Intelligence Studies Section of the International Studies Association. A prolific author on aspects of intelligence analysis and analytical theory, he is on the editorial board of the journal Intelligence and National Security. Before his academic career began, he spent five years as an analyst at the Central Intelligence Agency (CIA) and the U.S. Government Accountability Office (GAO):*

Intelligence analysis processes will undergo significant change over the next 10 years, while also retaining significant continuity. The continuity in intelligence analysis processes is a byproduct of its orientation to knowing and understanding, and the epistemological foundations for doing that —from historical to socio-cultural to philosophical to scientific—have not changed much over the centuries. At the same time, intelligence analysts are interposed between the changing nature of the kinds of information available to be collected, and the changing requirements of the decision makers. Advances in technology as well as the impact of technology on decision platforms and timeframes significantly affect the kind of information analyzed as well as the speed and format of delivery. The degree to which these advances in technology affect intelligence analysis depends on the kind of analysis being done (strategic, versus tactical, current versus future, threat actor versus environment, etc).

Because there are many different kinds of intelligence analysis, some will be radically different in 10 years while others will be much the same as they are today. The degree of impact of technology on analytic processes is dependent on the kind of analysis that is being done, and the respective ratio of data to concept that drives the inferences obtained. The greatest potential for change is likely to result from growing applications of automated analysis driven by artificial intelligence. If artificial intelligence is able to produce valid and reliable inferences, that has the potential to radically reshape both analytic production and consumption, particularly if tools enable consumer exploitation of the automated assessments.

Michael Warner *serves as an historian in the US Department of Defense. The views he expresses are his own and do not necessarily reflect official positions of the Department or any other US Government entity:*

Ten years from now the intelligence analysis that matters will be very different, yet much the same. It will be different because of its technology and its targets; it will be similar because the decision makers whom it serves will still wrestle with the same sorts of problems that they want analysts to analyze today.

Technology is transforming aspects of intelligence analysis, particularly the tools with which analysts can spot patterns in enormous data sets and extrapolate future trends from those correspondences. The sheer size and availability of such data sets is also increasing the demand for analysts who understand what those data sets represent – i.e., analysts who can answer questions like Where did the data originate? Who or what created them? Who collected them, and how? What can they show, and what can they not prove? And, very importantly, what legal restrictions and ramifications follow from our analysis of them?

Intelligence analysis will not change in that even the analysts who master Big Data will still need to express their conclusions to busy decision-makers in ways that are not only timely and coherent but evoke the trust of their "consumers" (or better yet, "clients"). Even the most technically specialized of analysts will still need to write clearly, to brief with coherence and conviction, and to collaborate with fellow analysts, collectors, and other colleagues. The constant need for the first two qualifications -- superior writing and speaking skills -- should be self-evident, although sadly it cannot be assumed in either government or academia. The latter qualification -- the willingness and ability to work in a collaborative manner with teammates, co-workers, experts, and superiors -- will only become more imperative as the speed and volume of analytical tasks increases.

David Kamien *is the CEO and Founder of Mind-Alliance Systems. Mind-Alliance designs knowledge systems and analytical methods that help managers cope with unpredictability by incorporating intelligence into decision making, strategy development, planning and forecasting. Trained as an attorney, Mr. Kamien has provided strategy, knowledge management, and research support to law firms, government regulators, and organizations such as Squire Patton. Boggs, Ogletree Deakins, NATO, the Rockefeller Foundation, the World Bank, the U.S. Department of Homeland Security, Raytheon, and the Center for Strategic & International Studies. He is the editor of The McGraw-Hill Homeland Security Handbook (2005, 2012 editions), and is the inventor of a patented information sharing planning method and system. A dual U.S.-Israeli citizen, Mr. Kamien served as an infantry officer in the Israel Defense Forces:*

Policymakers and executives will continue to routinely task their intelligence organizations with answering fast-turnaround intelligence queries focused on relatively short time frames. Analysts will spend so much time preparing for and attending meetings, as well as writing short response memos that it will remain difficult for them to free up time for strategic intelligence analyses.

Frameworks for prioritizing intelligence efforts will need to support more frequent updates that reflect daily changes in world events and policymaker priorities. Intelligence agencies will benefit from longer lead times in identifying emerging intelligence issues. They should always be proactive and have a ready answer to a question frequently asked by policymakers: "What should I be most worried about tomorrow, and why?"

As Artificial Intelligence (AI) technology improves, people will likely spend more time chatting with bots. They will come to expect software to do "low level" analytical tasks and free up time for sophisticated analysis, discussion and coordination with colleagues and partners. Unfortunately, this is unlikely because the sources and varieties of Data will increase faster than analytical capabilities. Meanwhile, intelligence customers will expect intelligence analysis (IA) organizations to anticipate their requirements and to deliver dynamically updated intelligence products, which means that analysts will remain under immense time pressure.

Anticipatory Intelligence will not only look at particular events that might occur, trying to achieve "foresight," but go further back and look at trends to help agencies and collectors position themselves. If analysts spot trends they think are critical and agencies do not have relevant collection or analytic capabilities (e.g. expertise), they can highlight areas where collection and analysis gaps must be closed.

Intelligence agencies will strive to develop the capabilities to more accurately anticipate, with longer lead times, real-world events, and the issues about which policymakers are likely to need intelligence support. An increasing number of organizations will build models and knowledge graphs in an effort to guide analysis and generate predictions based on patterns in data (e.g. disease outbreaks and civil unrest). They will need to grapple with a much larger spectrum of knowledge sources from both within and outside their organizations.

Changes in intelligence education and training are more and more necessary as a result of the analysts being expected to be become savier about data analytics and SATs. Thus, we expect to witness an increasing use of intelligence analysis training tools that can provide quantitative and qualitative feedback to students. Tools like *MindPeer* (http://www.mindpeer.com) will become part of the intelligence studies curriculum to help students learn how to think critically and cope with the challenges of Big Data.

Carmen Medina *is a former CIA Deputy Director of Intelligence. A 32-year veteran of the Intelligence Community, she is also the author of Rebels at Work: A Handbook for Leading Change from Within:*

When the real impact of the internet began to be felt in the early years of this century, I worried that political, economic, and social institutions would fail to keep up with coming changes. The flow of information was more voluminous, volatile, and, I thought most significant, more vulgar. I use the word vulgar in the way the ancient Romans did - to mean common and colloquial. Before the internet, information was elite-driven. Now information is controlled by everyone; people are free to believe what they want and to live in whichever echo chamber they choose. Unless intelligence agencies do a better job of adapting to these conditions, I fear they will suffer the same fate as other organizations tumbled by new social dynamics. To survive and perhaps even prosper, they need to change much of what they do so that they are better able to track all social groups, not just elites.

Current intelligence sources and methods are really about keeping tabs on what powerful people are doing. What do senior people in the government think? Who are the economic kingpins in country Y? But in a more "vulgar" society, things that matter are much more likely to occur bottom up. Unless you monitor the sentiments and narratives throughout society, you are likely to overestimate the strength of existing elite structures. And you'll be surprised when these elites lose influence and power. If intelligence organizations are thriving ten years from now, they'll have adapted by doing much more with Open Source Intelligence to keep track of popular sentiment in countries of concern. This will pose many challenges to existing tradecraft. Traditional sources and methods are designed to answer specific intelligence questions. But the world of open source is random - to harvest insight, intelligence analysts will need to ask novel and imaginative questions of the data and be prepared to pursue many dead ends. This will also require a new approach to the management of intelligence, which I suspect will pose the bigger challenge.

Randolph Pherson*, President of Pherson Associates, teaches critical thinking and advanced analytic techniques to analysts throughout the Intelligence Community and the private sector. Mr. Pherson completed a 28-year career in the Intelligence Community in 2000, last serving as National Intelligence Officer (NIO) for Latin America. Previously, at the CIA, Mr. Pherson managed the production of intelligence analysis on topics ranging from global instability to Latin America, served on the Inspector General's staff, and developed and implemented a strategic planning process for the CIA as Chief, Strategic Planning and Management Staff under the Deputy Director for Planning and Coordination (ExDir):*

The coming decade will be marked by increased globalization, more complex

geopolitical systems, persistent strains of nativism in many parts of the world, and technological change that many citizens will find overwhelming. Efforts to explain and track these trends will pose ever mounting challenges to the intelligence profession, but the greatest challenge may turn out to be one of process not substance. A major new concern for intelligence analysts will be knowing if what they are reading or seeing is true or whether someone—usually for ulterior motives—is purposively broadcasting untruths. Soon, the retort: "What can I believe anymore?" will ring increasingly in our ears.

Many of us have only recently recognized that we are living a new era of "Fake" and "Fraud" news as exemplified by Russian attempts to manipulate popular perceptions and inject false stories into the news streams of countries about to hold national elections. Lacking a massive—and unlikely—global campaign to ensure greater veracity in the distribution of news over social media, the transition to the Information Age will be marked by the need to make sense from a growing cacophony of competing, "alternative facts."

Similarly, we should anticipate a parallel onslaught of "alternative images" as technology, for example, now can generate videos of people appearing to vocalize words they never actually said. A successful campaign to counter this phenomenon would require the development of new technologies and procedures by global corporations such as Facebook, Instagram, and Twitter to vet what is distributed on the internet. If this fails, the stage could be set for an alt-internet to emerge that only contains data and images that have been vetted and can be trusted. In the Age of Information, the disciplines and traditions of intelligence analysis will become increasingly valued.

Dr. Dennis A. (Wes) Westbrooks II *is the Director of Undergraduate Studies at the National Intelligence University located in the Washington, DC metropolitan area. His writing and presentations primarily focus on intelligence studies but he has researched and written on numerous topics relevant to the Intelligence Community. Wes is a graduate of the National Defense University's Joint Professional Military Education program in Washington, DC and holds a BS from Hampton University, Hampton, VA, an MS from The George Washington University, Washington, DC, and a PhD from Hampton University, Hampton, VA:*

Intelligence analysis will not be different in 10 years despite technological advancements, the mission remains the same, to try to understand the future. My immediate thoughts go to the use of structured analytic techniques and Intelligence Community Directive (ICD) 203 Analytic Tradecraft Standards. The phrase "structured analytic techniques" was introduced to the United States Intelligence Community in 2005. These techniques are thought to reduce cognitive biases. ICD 203 was published in 2007 and was designed to guide analysis and analytic production. The United States Congress mandated these

analytic efforts in reaction to the shock of 9/11 and the subsequent incorrect claim of weapons of mass destruction in Iraq. Due to the amount of scrutiny by policymakers and the American public, the combination of the techniques and standards provide the Intelligence Community with a solid analytic framework.

Intelligence analysis is an ancient art that has changed very little in the history of mankind, in an attempt to understand our adversaries. Structured analytic techniques provide analysts with the requisite level of unambiguousness, objectivity, and forethought required to avoid strategic surprise. ICD 203 sought to codify the analysis process and improve analysis "tradecraft." Structured analytic techniques and ICD 203 are still used in intelligence analysis more than 10 years later and it is my opinion they won't be much different in 10 years.

Intelligence analysis will be slightly modified to some degree but will remain fundamentally unchanged. The fundamental challenge is to make sense of the forest of information that modern technology provides intelligence analysis. We teach these techniques and standards to our students as a systematic way to solve a problem. The techniques coupled with the standards help our students achieve analytic rigor and academic excellence with the understanding that the best we can do is reduce uncertainty and not predict the future.

Erik Elgersma *is Director of Strategic Analysis at FrieslandCampina. Experienced Strategic Analysis Director with a history of working 35,000 hours in the dairy industry. Author of two authorative books on market intelligence: The Strategic Analysis Cycle Handbook resp. Toolbook. Skilled in Global Business Strategy Design and Execution, Dairy Business, B2B Chemicals . Strong business development professional with a Doctor of Philosophy (Ph.D.) Chemical Engineering from Delft University of Technology, alumnus of International Institute for Applied Systems Analysis (Vienna). Executive education at Harvard Business School, Insead, IMD, London School of Business and Jane's Military Intelligence. Guest lecturer at Brunel University London, HAS Den Bosch, Netherlands, Vlerick School of Business, Gent, Belgium:*

The table below based on the classical concept of the intelligence cycle may help answering the question.

In summary:

in briefing:	a higher work pace, less long-term planning, more 'tyranny-of-current-intelligence'.	
	in collection:	permanent and actual access to the data of the whole world in collection, with ever better tools to discern 'need-to-know' data from useless false positives.

Intelligence cycle phase	around 1997	around 2017	around 2027
Requirements	70% annually planned 30% ad hoc requests	40% annually planned 60% ad hoc requests	20% annually planned 80% ad hoc requests
Collection	OSINT: mainly paper sources, some internet, weekly or even monthly 'news' cycle; single dimension metadata; single of maximum a few languages HUMINT: interviews based on paper-based question lists	OSINT: 95+% internet-based, real-time sources. 24/7 'news' cycle; multi-dimension metadata-supported searches, language by language HUMINT: real-time face-to-face interviews (Skype…); occasional crowd sourcing, online questionnaires etc	OSINT: 98+% internet-based, real-time sources. 24/7 'news' cycle; multi-dimension metadata-led searches based on 'natural language processing' in multiple languages HUMINT: real-time face-to-face interviews (Skype…); broad, fast, automated application of e.g. social media-based crowd sourcing, Delphi method-based forecasting, etc.
Analysis	Mainly critical thinking, supported by single-user, basic tools and PC-computing power	Still critical thinking, supported by AI-based forecasting tools (data science) especially in quantitative fields	Analyst' critical thinking, led by AI-based forecasting tools (data science) – 'IBM Watson'-style.
Reporting	Hard copy reports formally sent to management; occasional live presentation	Powerpoint and Word documents unless; occasional live presentation. Initial use of videos as reporting tool	Videos as reporting tool, powerpoint and word document at best as back-ups
Knowledge management	Hard copy filing in one location, led by metadata dimension (e.g. company name), perhaps a few shared excel databases, monthly updated by a single administrator	90% automated, daily updated, multiple dimension metadata-based, globally 24/7 accessible knowledge house, offering a few languages, with central own-company administration team	98% automated, permanently updated, multiple dimension metadata-based, globally 24/7 accessible knowledge house, offering dozens of languages, with central but outsourced administration team

in analysis:	from single analyst (team) prerogative to servant of superior computer (AI-) power, with "IBM Watson"-type tools in the role of the new Delphi oracle and the analyst as the priest-interpreter towards 2027's kings (i.e. business management).
in reporting:	from paper via powerpoint to real-life videos, with the ever greater risk that visualization and dramatization skills matter more than solid analysis-based conclusions. Analysts as actors and AI-priests, rather than as independent thinkers.
in filing:	from single site, single language, single metadata-dimension 'archives' to globally 24/7 accessible multiple-dimension, permanently actualized data warehouse in multiple languages.

Stephen Coulthart *is an assistant professor of security studies in the National Security Studies Institute at The University of Texas at El Paso. His research focuses on intelligence analysis and illicit networks. He holds a Ph.D. in Public and International Affairs from the University of Pittsburgh as well as two master's degrees in international relations and public administration, both from Seton Hall University. While at the University of Pittsburgh, he received the Harold D. Lasswell award from the Horowitz Foundation for his dissertation research on analytic reform in the U.S. intelligence community:*

Intelligence analysis in 2020 will be shaped by two factors: the unpredictability of international events and the increasing power of data storage and analytics. In recent years, a number of international events caught decision makers by surprise like the Arab Spring. These geopolitical disruptions will persist and intelligence agencies will bear the brunt of public criticism for not warning about them.

At the same time, digital technologies will reliably improve as they have done for decades and wealthy states will look to these "big data" fixes in the hopes of foreseeing disruptions. In some cases, these technologies will improve situational awareness but the human-in-the-loop will remain an important ingredient. Why? Because while computation will improve significantly in the next 10 years, it will not come close to replacing the human analyst; modelling human creativity is still beyond the technological horizon.

In 2020 then, as today, the symbiosis between humans and computers will continue to grow. In concrete terms this means the typical analyst will have

the traditional subject matter expertise on security threats or regions but also increasingly have the skills of a computer scientist (e.g. write code) or at the very least be able to understand technical details (e.g. read code).

Jorhena Thomas *is currently a Lecturer in the Applied Intelligence Master's Program at Georgetown University in Washington, DC. She has extensive experience in intelligence analysis, homeland security, and public safety at the international, national, and local levels. Jorhena has also served as Principal Consultant at Wright Thomas International; Chief of Staff to the District of Columbia Deputy Mayor for Public Safety and Justice; Deputy Director at the Washington Regional Threat Analysis Center (the District of Columbia's intelligence fusion center); and Senior Intelligence Analyst with the FBI:*

When I think of how Intelligence analysis will evolve over the next decade, three things immediately come to mind:

1) The type of people who will be analysts:

We will see a wider variety of people entering the field, and not for lifelong careers. Economies throughout the world are seeing workers change professions several times in a lifespan, much more often than in past generations. The intelligence analysis realm is not immune to this generational shift, nor should it be. The moving of people with solid analysis skills among the military, civilian government, law enforcement, and private sector analysis communities is a healthy evolution, and one that will positively impact intelligence analysis in the next decade. This movement will give diversity of thought and the application of fresh ideas across sector boundaries.

2) The resourcefulness of the job:

Intelligence analysis will become more resourceful over the next decade, and the incorporation of nontraditional partners will continue. Look at how much more resourceful the US Intelligence Community became after 9/11. The federal government immediately saw the need to share and receive intelligence from a broader range of entities. This will continue across the spectrum of analysis disciplines in the next decade, as the idea of fusion intelligence practices takes hold around the world. Along with this will be increased reliance on OSINT (open source intelligence) and the introduction of new -INTs to the core categories.

3) The one thing that won't ever change:

Critical thinking by humans has been and always will be the driving force behind effective intelligence analysis. That won't change. Although powerful computers, fancy analytic tools, and advances in artificial intelligence might make the work easier, they won't replace people.

Garry Clement *is a Financial Crime Prevention expert and advocate, who joined the Association of Certified Financial Crime Specialists team in 2016*

as the Executive Vice President. Garry brings over 25 years of financial crime fighting experience. Mr. Clement relies on his 34 years of policing experience, having worked in roles as the National Director for the RCMP's Proceeds of Crime Program, working as an investigator and undercover operator in some of the highest organized crime levels throughout Canada. During Garry's policing career, he received numerous awards and commendations for his investigative abilities, inclusive of recognitions from the US Drug Enforcement Administration and the CIA:

Looking ahead 10 years and anticipating the future of intelligence and its application to fulfil the duty of care for citizens offers both excitement and new challenges. We are going to be a world of connections and have the capacity to manage mega-data through the evolution of artificial intelligence (AI). Such AI techniques as vision, speech, and gait analysis will add to a new dimension to the intelligence community and aid in interviewing/interrogating and the ability to detect deception with far more accuracy than exists today. Additionally, we will be working in an environment where AI will reduce human biases and false assumptions.

In a world that embraces the internet of things we will have access to droves of open source information, video surveillance will continue to evolve to protect our societies, from streets to hospitals to airports and our world will function primarily through electronic means. Some cities have already added drones for surveillance purposes, and police use of drones to maintain security of ports, airports, coastal areas, waterways, industrial facilities are likely to increase, raising concerns about privacy, safety, and other issues.

Criminals and rogue states will embrace what technology offers and will continue to capitalize on the fact their territory is the world, unencumbered by a country's sovereignty. These actors will continue to capitalize on their freedom and agility to adjust and reap the benefits of what technology and open source material offers.

Successful intelligence operatives and organizations will value international partnerships and embrace modern technologies as they are developed not letting bureaucracy hinder success. A successful model will be the prioritization of broad-based knowledge sharing and coordinated priorities across industry stakeholders i.e. It will take a network to defeat a network. Professionals, practices and industry constituents will need to evolve so that Impactful Disruption can be achieved.

The biggest challenge for anyone in the intelligence world will be embracing the notion of ongoing learning and accepting technology for what it offers.

Martin Bang *works at the Swedish National Defense University. He is a non-commissioned officer in the Swedish armed forces and has a Ph.D. in*

Military Science. His research interest is military intelligence and particularly in analysis and the role of the institution:

If we focus on the changes within the area of intelligence analysis, I believe the main changes we are going to see in 10 years are connected to what can be called the evolution of data processing. An ever-increasing data and information volume has been considered as a problem for a long time within the intelligence community. However, the possibilities with massive collection in the cyber arena, both open source as well as more covert cyber collection, increases this further. In addition, the computer added solutions to this problem have matured rapidly during the last couple of years. There is an abundance of concepts connected to this: deep learning, big data, datamining/farming, just to mention a few. The possibilities are great and real, but not without pitfalls.

Intelligence analysis can enter two different paths in this respect. One in which the computer aided information producing works as a catalyst for the analysis. The other possible path is less positive where the developed tools start directing what type of questions the intelligence service seek to answer and thereby limits the intelligence analysis. A worst case would imply that the evolution of data processing drive intelligence analysis to merely information analysis.

Ralph D. Sawyer *is an independent historical scholar and strategic consultant to government agencies and international corporations, specialized in Chinese military issues for five decades. His numerous books include three highly regarded intelligence studies: The Tao of Spycraft: Intelligence Theory and Practice in Traditional China; The Tao of Deception: Unorthodox Warfare in Historic and Modern China; and Lever of Power: Military Deception in China and the West:*

Several trends will make the task of assessment infinitely more complex. First and foremost, the Internet's geometrically expanding exploitation will facilitate the dissemination of a myriad "stories," all purporting to be reports of actions, developments, and intentions. Reflecting multiple perspectives and nefarious motives, their sheer weight will create a sort of "truth by numbers," distracting attention from crucial issues and constraining interpretive possibilities. Naïve faith in the veracity of massive data crunching and cloud based analysis will further exacerbate the problem.

Successfully penetrating the noise of this radically distorted landscape will require perspicacious, supposedly "objective" onsite observers who will inevitably struggle with inadequate cultural knowledge and be affected by their own heritage and expectations. This will place a premium on informants and defectors, raising the full continuum of problems associated with disinformation, misdirection, manipulation, and obscuration. "Real information" will therefore acquire a much more "accidental" nature,

complicating analysis greatly.

While capabilities can be expected to remain reasonably transparent because of space based observation platforms, intentions will probably become more opaque due to the re-emergence of dictatorial leaders. Their paranoia, penchant for secrecy, and blustering and posturing, coupled with the increased prominence of internal issues in shaping external actions and an ongoing failure to fully comprehend the calculus of other value systems will make fathoming intentions and predicting actions far more difficult, especially if agencies assume rationality and self-interest should prevail.

Finally, while the sheer number of transmissions would seem to ensure a greater database for scrutiny, intercepts of any value will increasingly diminish due to increased use of complex encryption methods, avoidance of susceptible means of communications, and widespread installation of fiber-optic cables. Cleverness will become the watchword of inimical organisations, resulting in a pronounced disjunct between the visible and intended.

Antonia Colibasanu *is a senior geopolitical analyst, focusing on strategic competitive intelligence analysis. She has joined Geopolitical Futures team as Senior Analyst in 2016, after working for more than 10 years with global analysis firm Stratfor in various positions. She works closely with bestselling authors George Friedman and Robert D. Kaplan and served as Honorary Adviser to Romania's Minister of Energy. Dr. Colibasanu was an associate professor at the Romanian National Intelligence Academy and Bucharest University. She is an alumna of the International Institute on Politics and Economics, Georgetown University. You can contact her at http://www.colibasanu.ro/project/antonia-colibasanu/ :*

Intelligence, in its most basic form, gives government and business leaders actionable information to make decisions, develop and support strategies. Governments' strategies are designed on the national interest foundation, while businesses strategies relate to profit. Nothing will change in this sense. What will change, however is the way intelligence analysis is done and what it takes into consideration.

There is the perception that the internet facilitates access to more information, which, in turn, makes intelligence analysis more difficult. Automated processes will increasingly be needed to manage the information overload, differentiating noise from usable data and transforming it into information. In the same time, sensing propaganda and fake data within the noise launched on the masses is likely to be increasingly automated considering that the public has traditionally been the subject for information warfare and the internet only intensified that.

Global disintegration into distinct social communities, both within the nation

states but also active at transnational level, as their formation has been facilitated by increased digitization, poses new challenges to the intelligence community. This phenomenon will require of national intelligence agencies both to cooperate with their counterparts and also focus on tackling specific challenges at the local level, in a competitive way, to address such communities-related problems. Businesses need to understand such developments in addressing both new and existing markets. Activism or conscientious consumerism making use of social media and other means of communication to influence consumers is just an example directly affecting businesses worldwide.

The main challenge for the intelligence community in the next decade will be asking the right questions when it comes to assessing the effects of technological progress on humanity at large and on their customers in particular. Digitization, in a sense, belongs to the past and will be managed in an increasingly efficient way. But technological systemic evolution that refers at phenomena such as cyberattacks, cryptocurrencies' parallel financial systems, the potential invention of high energy lasers for new military weapons, all influence citizens directly. The intelligence community will need to become more sophisticated in dealing with all these – separating what will potentially affect its customers (the citizens), when and how that will happen and what will not.

Major Lars C. Borg *is a researcher and instructor at the Norwegian Defence Intelligence School, Centre for Intelligence Studies. Major Borg has more than 20 years' experience from the Norwegian Armed Forces, working with intelligence from a tactical to the strategic level, at home and abroad. In addition to his military education, he holds a master's degree in War Studies from King's College London. Borg is currently working on a PhD at Brunel Centre for Intelligence and Security Studies, Brunel University London:*

Intelligence analysis for tomorrow will hopefully follow in the path of medicine by ending "the God complex" of the old-fashioned subject-matter experts and realise the need for a more scientific approach. Consequently, what Tetlock named Hedgehogs will then be replaced by foxes, people who can tackle any intelligence problem, not just the one. Intelligence analysis will be a field for Superforecasters; creative and critical thinkers with a liking for Bayesian reasoning.

Artificial Intelligence (AI) will take over for the subject-matter experts when it comes to create improved past and present state models, patterns, trends, and driving forces related to the intelligence problems. However, as AI has yet to develop human creativity, the role of the analysts will be increasingly important, meaning one must turn away from single-outcome analysis to rather work with alternative scenarios, bordering the known uknowns, entering into the territory of wild cards and black swans.

Intelligence analysis will in lesser extent be viewed as an art, but more as an approximation to science with an increased focus on an audit trail. Nevertheless, predictive accuracy will be hard-found as decision-makers acting on good intelligence warnings will make predictions void.

Adam D.M. Svendsen *is an intelligence & defence strategist, educator, researcher, and consultant. He holds a PhD from Warwick University, UK.* *http://orcid.org/0000-0002-0684-9967* **| *twitter:*** *@intstrategist :*

Current intelligence analysis 'professionalisation' processes can be readily anticipated to extend further into the future. As Professor Allyson MacVean has argued: "It is widely accepted that a profession can be defined as occupations that embrace six particular features: *autonomy, commitment, collegiality, extensive education, service orientation and specialised skills and knowledge*." Moreover: "[F]irst is formal higher education to provide basic knowledge and skills. A profession will have its own core curriculum that teaches advanced theory and practice… [S]econd is professional socialisation, where practitioners adopt the values and culture of the occupation formally and informally, and as a member of the occupation identify with its ethics, principles and standards." (Svendsen, 2012. pp. 7-8)

When philosophising about future intelligence analysis, rather than solely increasingly adopting and implementing those above 'professionalisation' features - albeit, at times, perhaps more haphazardly than smoothly and/or incrementally - intelligence analysis will also intimately involve more building and synthesis activities pertaining to the wider and deeper-ranging assessment and estimate-related queries of '*why?*', '*so what?*', '*what does it mean?*', and so forth. Much demanded by commanders and other decision-makers, those sense-making activities will go beyond merely more 'breaking-down' (disaggregation) activities that are traditionally associated with analysis when striving to answer the classic '*what is it?*' questions. That movement will occur particularly as greater '*Intelligence Engineering*' is advanced. (Svendsen, 2017)

Giliam de Valk *is a professor at Leiden University. He has lectured at various academic institutes on intelligence, intelligence history, military strategy, counterinsurgency and counterterrorism. He wrote his PhD on the Quality of Intelligence Analysis [2005] and is currently focusing on the methodology on how not to miss threats:*

Shifting risk and threats will call for a new methodological paradigm for intelligence analysis. Whereas traditional risk-based analysis focuses on events that are known to the intelligence analyst, the importance of unknown threats is growing very swiftly. Instead of assessing risks, therefore, intelligence analysts will have to make sure that they do not overlook threats. In methodological

terms, from reducing the α (the chance of incorrectly inferring relationships), intelligence analysis will be designed to reducing the β (the chance of not missing relevant relationships).

Although we see that practitioners are trying to adapt to this new situation, the underlying theoretical and methodological framework is largely lacking. Academics have reflected on how the α can be reduced through inductive, deductive, and abductive reasoning, but how logic can reduce the β has not been explored at a fundamental methodological level yet. This will have consequences for the research design: tooling is needed to take into account the unknowns, not only to collect the relevant data, but also in order to choose and develop the adequate methods.

Since the public and political expectations vis-à-vis intelligence and security services are extremely high, most notably in the domain of counterterrorism, we expect that the methodological research needed to provide analysts with proper frameworks will catch up in the years to come.

Irena Chiru *is Director of the National Institute for Intelligence Studies within the "Mihai Viteazul" National Intelligence Academy, Romania. She is also a regional editor of the International Journal of Intelligence, Security, and Public Affairs, member of the editorial board of the International Journal of Intelligence and Counterintelligence and of the Romanian Journal of Intelligence Studies. In the last 6 years, she has been the organizer of the Intelligence in the Knowledge Society, an international conference that has become a landmark event in the field of security and intelligence studies bringing together academics and practitioners from all around the world. She is the author and co-author of several books, chapters and articles focused on intelligence and communication:*

The last decades have brought forward significant and accelerated technological developments which, in their turn, have generated opportunities for intelligence services but also threats against international and national security. Therefore, any exercise of imagination into the future of intelligence analysis starts form a "double-edged sword": the data abundance has come with the negative corollary of a poverty of attention, the complexity of the current security setting has made the full spectrum of consequences hard to predict and intelligence organizations, although more technologized than ever, have been struggling with the need to continuously adapt and rapidly perform.

History in general and intelligence history in particular have proven that most of the lessons we needed to learn had already been taught in the past. Starting from this premise, my scenario will dwell on the Aristotle's "Golden Mean" and on the principles of symmetry, proportion, and harmony. It is my conviction that the key to understanding and preparing for the future of intelligence analysis resides in a shared attempt to find the best of the possible balance between the contradictory and competing forces that are presently impacting the universe of intelligence analysis:

- Past – Future

For intelligence analysis to preserve its competitiveness in a volatile and convoluted security environment, it needs to look into the past, review its core values, lessons known and lessons learnt. It also needs to look ahead, exploring the "what ifs" and preparing to be the first to capitalize on the change future will bring. It would be a dangerous delusion to envisage the future of intelligence without properly understanding and embracing the past.

- Successes - Failures

In intelligence, the rule of the thumb is to avoid failure by anticipation and keep the secret of successful operations. However, intelligence organizations are at their turn the expression of various variables (human, time, doctrine, strategic culture etc.) which may lead to imperfection and implicitly to failure. Commonly, failure tends to be more public than success, which in the case of intelligence involves particular reverberations with high stakes. There are only few intelligence services which have so far understood that failure is the seed for growth and even fewer which understood the need to integrate "failure capitalization" as part in the internal analytical culture.

- Mind – Technology

For years, the best analysis method has been the intelligence analyst, bringing value added through creativity, curiosity, open mindedness and critical thinking. However, one has to be naive not to take into consideration the technological developments entailing the use of new instruments that automatize analysis while progressively challenging the long-lived general accepted leading role of the analyst. Will artificial intelligence correct the inherent errors in the intelligence analysis profession? It definitely impacts it and consequently analysts need to adapt and learn how to integrate new technologies in the process while remaining vigilant to the dark side of technology and connectivity.

One simple but impactful manner in which we can define intelligence analysis is to look at it as the process of providing answers to smart and structured questions. Accordingly, the future of intelligence analysis depends on the agency of intelligence organizations to provide the right answers and solutions to the difficult and vulnerable equilibrium between past and future, success and failure, human and artificial intelligence.

***Avner Barnea**, Ph.D. is a senior competitive intelligence strategic consultant, teaching strategic CI in various MBA programs in the academia in Israel. He is the head of the special program on competitive intelligence, corporate security, cyber security and crisis management in the MBA program at Netanya Academic College, in Netanya, Israel. Dr. Barnea is also a former senior officer with the Israeli Intelligence Community and currently chairman ofthe Israel CI Forum (FIMAT) and member of SCIP Board of Directors. He is a*

research fellow, National Security Studies Center, University of Haifa, Israel:

There will always be a gap between the need to know and the information in hand, making assessments the core challenge of the analytic process. Since the recent progress of Artificial Intelligence (AI), it looks as if a new opportunity is coming up. Using the latest capabilities of AI seems to be a wonderful tool for the Intelligence Community (IC) to upgrade the quality of analysts' reports.

Presently, AI capabilities can provide intelligent learning algorithms, able to analyze data, draw conclusions and even recommend the best solutions. In addition, AI has the ability to build predictions based on incomplete information. For instance, predictive analytics can be used to map a complex decision tree of all possible outcomes, which will then simplify human decision-making. AI can perform tasks such as identifying patterns from a large amount of data more efficiently than humans, enabling businesses to gain more insight out of their data.

Intelligence agencies in the US, UK and Israel have already started to look carefully into further developing these AI opportunities. Dawn Meyerriecks, the CIA's deputy director for science and technology, announced that "The CIA currently has 137 pilot projects directly related to artificial intelligence." Nevertheless, as officials explain, despite the great amount of investment in AI capabilities, they will not lose sight of the importance of the human analyst. Melissa Drisko, the Defense Intelligence Agency's deputy director, pointed out that "As we're looking at algorithmic analysis, artificial intelligence, machine learning, we're finding [that] we're having to examine what the role [is] of the human and the analyst."

What are the expectations of these intelligence organizations in the coming age of AI? As I can see from the Israeli perspective, the use of AI in the intelligence analysis, both for business and government is seen as an opportunity that can consolidate the ability to predict future moves by key competitors and enemies. As a result, many corporations are allocating and will continue to allocate significant resources to gathering and analyzing massive amounts of information about their rivals. Moreover, predictive analytics tools will be developed to reduce surprises and avoid failures, and further training of analysts will be adapted in order to meet these challenges and facilitate the work with these

Intelligence and International Relations: a Much-Needed Future Dialogue

Mitterand M. Okorie *is a Conflict Transformation and Peace Studies (CTPS) Doctoral Candidate at the University of KwaZulu-Natal, Durban, South Africa. He holds a MSc. in Terrorism and International Relations from Aberystwyth University, United Kingdom and a B.A in International Relations from Eastern Mediterranean University, North Cyprus. Between 2015 and*

2017, he taught Peace & Conflict Resolution at Michael Okpara University of Agriculture Umudike, Nigeria. Email: mitterandokorie@gmail.com:

The military campaign by Nigeria to combat the Islamic militant group Boko, Haram has suffered a fatal blow with the country's new strategy of establishing fortress towns. These towns, one of them—Bama (second largest town in Borno State), would act as garrison encampments to house those displaced by Boko Haram. This, it is expected, would provide opportunities for the displaced to rebuild their lives and forfeit the hope of ever returning to their homes. In effect, the Nigerian military is prepared to fortify already held territories than commit more soldiers to the frontlines to retake the territories held by the insurgents.

This tacit forfeiture of Nigerian territory to Boko Haram clearly exemplifies the catastrophic failure of intelligence by the country's Intelligence Authorities. There are reports that the lack of intelligence sharing between Nigeria and neighbouring countries, like Niger, Cameroon, Chad, and Benin has incapacitated the counter-insurgency efforts and weakened the possibilities of an effective regional response to the Boko Haram threat.

Yet, it is not so much the problem of intelligence sharing as it is that of intelligence gathering. It would be impossible to share intelligence if one does not gather it. For instance, while military efforts have freed thousands of hostages from Boko Haram (especially since 2015), there seem to be very little information gathered from these former Boko Haram hostages. If there was, there certainly is no evidence that these insights have provided any tactical advantage as to locating insurgent hideouts, or disrupting their movements around the borders with neighbouring countries. Boko Haram is in fact, stronger than it has ever been, given their ability to plan and execute attacks on hard targets.

It is important to point out that, in much of West Africa, the post-independence national security architecture has been exclusively restricted to forestall the outbreak of civil wars or coup d'état. The institutional weakness and corruption in these security bodies have guaranteed only protection of the elite in power more than the society at large. Against this background, intelligence gathering that protects the nation is underplayed, while resources and manpower to protect the regime elites intensifies. It is a crying shame for instance that the official website for Nigeria's Defence Intelligence Agency (DIA) has no information about its "Mandate" and only records a single sentence about its "Vision" and "Mission". This undoubtedly is one of the tragedies of public and security institutions in much of postcolonial Africa.

As unfortunate as it appears, the Nigerian government has adopted the building of fortress towns in Borno state to permanently resettle citizens displaced by an insurgency which it has failed to dislodge for more than 8 years. And for this, the lack of actionable intelligence from within Nigeria, and from other border countries is highly responsible. For Nigeria, and much of postcolonial Africa,

counter-insurgency intelligence gathering still represents an ominous blind spot in their security architecture.

What then is the fate of intelligence in West Africa and the Sahel, given the palpable threat of Islamic militants and its destabilising ramifications for the region? As have been noted earlier, intelligence gathering capacities for countering the religious extremist groups within the region is currently weak, leaning mostly on the United States to assist in this regard.

Against this background, it is fair to suggest that the possibilities of an improved intelligence gathering capability in West Africa would be critically dependent on U.S military assistance, and the extent to which providing this assistance remains relevant to U.S' strategic interest. In recent times, the U.S has continued to sponsor and coordinate an annual counter-terrorism exercise known as "Flintlock" (currently in its 11th edition)—which trains military personnel within the West African region on how to use the relevant technology to communicate between cellphones, radios and computers with respect to joint counter-terrorism efforts. The Flintlock exercise would also involve the U.S. military introducing a "cloud-based" technology to allow African allies to quickly share intelligence across borders, such as mapping information on the location of potential target.

This however raises concerns about questions of territorial integrity within the African continent, given the possibilities that U.S intelligence gathering technologies could still be used to gather intelligence of these sovereign partner nations. And for how long is the dependency on the U.S or developing intelligence gathering capability lasts? There has to be an exit strategy for these countries at some point—as far as developing an effective and self-sustaining intelligence gathering capacity. That possibility, however, appears to be distant.

Co-Editors' Perspectives

Daniela Bacheş-Torres *is a Ph.D. candidate at Brunel University in London, with a focus on intelligence cooperation in the European Union. She has worked as an assistant researcher at the "Mihai Viteazul" National Intelligence Academy in Romania where she was largely involved in the research projects conducted by the National Institute for Intelligence Studies. Ms. Bacheş was a member in two European projects: "Setting-up an Air-Marshal Training Center – ARMLET" and "Citizens Interaction Technologies Yield Community Policing –CITYCoP".*

Within the next decade, the security environment will go digital, requiring institutional stakeholders to adapt their methods and tools. Concurrently, collaborative work – ranging from informal networks to strategic partnerships – will become a procedural framework meant to increase the empowerment of organizations and the effectiveness of goal achievement through the use of all-source intelligence.

On the one hand, Big Data and Artificial Intelligence (AI) will become the core of the analytic process aimed at identifying (Descriptive and Evaluative Analytics), predicting (Predictive Analytics) and assessing (Prescriptive Analytics and Complexity Science) trends that might influence future decision-making, competitiveness or outcomes. At the same time, the continuous proliferation of information will require innovative all-source analytic tools. This implies the development of software applications, analytics methods and algorithms that can help decision-makers understand and keep up with the high flow of data and information. To achieve their purpose, ICs (both government and private-sector ICs) will need to build complex analytic mechanisms able to efficiently combine AI and human resource capabilities. In addition, intelligence professionals (both analysts and collectors) must develop intelligence & knowledge management mechanisms to increase efficiency of intelligence products.

On the other hand, analysis conducted by both the Government and non-government sectors will move towards a more integrated working approach that will witness the passage from information sharing and competitive cooperation to joint operational planning and collaborative knowledge building. This evolution will happen not only within one organization or community of practice, but also across different fields of expertise and sectors of activity that need to face similar challenges (e.g. cyber-attacks). While increased access to a broader pool of resources will remain an important incentive, analysts will be required to master a wide range of tools and best practices from other sectors, as well as adapt them to their own needs and resources. Moreover, cross-collaboration among different agencies of the same IC, institutional actors from both private and public sectors, or even organizations from various countries will continue to develop not just for pulling together resources and intelligence, but especially for creating common knowledge.

Efren R. Torres-Bacheş *currently works as a senior regional intelligence analyst in the private sector with a main focus on drug cartel activity and tactics in Colombia, Ecuador, Venezuela and Mexico. Mr. Torres has an academic background in Intelligence and Security Studies, Strategic Studies and Terrorism. He has also studied Cognitive Psychology from the University of California, Irvine. The most recent degree obtained was a Masters obtained at Brunel University in London, where he developed his research on improving outcomes in intelligence analysis and medicine under the supervision of Dr. Stephen Marrin.*

All of the contributors have hinted at the increasing role of open-source intelligence (OSINT) and the issues of veracity of information found on the internet. That being said, my response to our question is two-fold. First, the role of OSINT, and the ongoing development of its collection gathering tools, will continue to increase in the years to come. Second, there will be a propagation of a new breed of intelligence analysts that speak OSINT as a native language and that place less

importance on covert sources and more importance on open sources as well as social media intelligence. Security threats and risks will likely remain the same; terrorism is highly likely to remain as the main threat that intelligence analysts in the private and public sector will continue to study and monitor. Overall, as we continue to evolve technologically in the era of information, all these threats will be augmented as information (good quality and poor quality) is within the reach of any individual for pious but also for nefarious purposes.

Despite the development of new tools for collection, intelligence analysis will, at its core, preserve its essence. Structured Analytic Techniques (SATs) will continue to be an important resource for analysts; the intelligence cycle will remain relevant; covert sources will continue to be an important staple of the IC; however, the biggest challenge for intelligence analysts in the next decade will be to deal with the complexity of information found in open sources. The amount of information gathered by OSINT analysts a decade from now will be facilitated by new collection tools developed by private technology companies such as Dataminr, which *allow the user to obtain high-impact events instantly and critical breaking information long before it's in the news* (www.dataminr.com). Access to real-time intelligence through similar platforms will shift the focus from HUMINT sources to a more crowd-sourcing approach that delivers important information at a faster pace. Notwithstanding, the speed in which analysts will be able to gather intelligence from open sources in ten years will pose a severe challenge; ranging from reliable sources to sources presenting information with the purpose of deception, intelligence analysts will need additional layers of questioning and vetting of every single bit of intelligence acquired through open sources. Despite the various new tools and methodologies that will emerge in the next ten years, the main challenge for intelligence analysts will be the difficulty in separating the signal from the noise, truth from lies, and news from "fake news" or half-told truths.

In the coming years, individuals wishing to engage in traditional intelligence analysis work will have more options outside of the military and government intelligence agencies. Future intelligence analysts are likely to look for opportunities in a more transparent environment. Less attention will be placed on the "secret" appealing and sexy side of the profession in government and more focus will be placed on the private sector for emerging opportunities that offer analysts the same type of work minus the bureaucracy. Since I started practicing intelligence analysis in the private sector, I have encountered many fellow analysts that rather enjoy the interesting, and sometimes secretive, nature of the intelligence work done in the corporate world, and I need to say, a good portion of these analysts have a poor opinion of intelligence agencies; they consider the clearance process long and tedious and to some degree unnecessary- let's be honest, no investigation is able to completely detect the next traitor such as Snowden. The next ten years will see this new generation of intelligence analysts

thriving in an open environment that emphasizes cooperation and collaboration with other like-minded private companies and also with government agencies. The private-sector intelligence analysts that I have met, some of which have transitioned directly from the United States Intelligence Community (USIC), have expressed their content with being able to freely move around and liaise with foreigners and other entities without counterintelligence concerns and without the necessary bureaucratic impediments from government organizations. Also worth noting, ten years from now, the national intelligence and private sector intelligence workforce will also be different as they will be led by this new generation of analysts that have a much different and fresher perspective than the obsolete Cold War Warriors still monopolizing the IC.

Lastly, a decade from now, let's hope that academia will be kind enough to be more interested in developing the intelligence studies literature by including the work done in the corporate world. It would be a complete disappointment to see academia miss opportunities to develop the literature in intelligence studies because it has become a victim of tunnel vision. By being a victim of tunnel vision, academics of intelligence are taking two steps forward and five steps backwards. Currently, academics cannot accept that intelligence can be applied outside the national security context. If academics, within the next ten years, do not adopt an all-inclusive cross-domain approach to develop the literature, and abandon the misconception that intelligence always equals secrets, then they are no better than the very entities they scrutinize for their intelligence failures. If academics do not adopt a proactive approach and step out of their comfort zone then many opportunities will be missed, and academia will keep running in circles chasing its tail. If this occurs, intelligence studies will sadly remain unchanged and underdeveloped in the next decade.

Drawing a near-accurate picture of what intelligence analysis will look like in the next ten years is quite challenging. Many elements may come into play: the development of new OSINT platforms and tools, future intelligence reforms, a new large-scale terrorist attack that is likely to re-shape foreign policy, and with that, the way that intelligence analysis is being conducted. We live in a complex world with even more complex threats. Perhaps the future of intelligence analysis lies somewhere in between all the ideas expressed here by all the contributors. Perhaps we missed important aspects and intelligence analysis will be much different than we imagined. Perhaps intelligence analysis will remain unchanged. Then again, we do not have a crystal ball; who can say where the road goes? Only time will tell.

ABOUT THE CONTRIBUTORS

Daniela Bacheş-Torres is a PhD candidate at Brunel University, UK, with a focus on intelligence cooperation in the European Union. She has worked as an assistant researcher at the „Mihai Viteazul" National Intelligence Academy in Romania where she was largely involved in the research projects conducted by the National Institute for Intelligence Studies. Ms. Bacheş was a member in two European projects: „Setting-up an Air-Marshal Training Center – ARMLET" and "Citizens Interaction Technologies Yield Community policing –CITYCoP". Ms Bacheş initiated and leads the Early Career Scholars Group, a junior scholars network under the Intelligence Studies Section at ISA. She is also an active member of the Intelligence Association for Intelligence Studies (IAFIE) and a Board member of IAFIE Europe, and is currently working on a project for developing a cross-sector intelligence analysis curriculum.

Efren R. Torres-Bacheş currently works as a senior intelligence analyst in the private sector with a main focus on drug cartel activity and tactics in Colombia, Ecuador, Venezuela and Mexico. Mr. Torres holds an MA in Intelligence and Security Studies from Brunel University, an MSc Econ. in Intelligence, Strategic Studies and Terrorism from the University of Wales, Aberystwyth, and a BA in Cognitive Psychology from the University of California, Irvine. The most recent was a Masters obtained at Brunel University in London, where he developed his research on improving outcomes in intelligence analysis and medicine under the supervision of Dr. Stephen Marrin. Mr. Torres also attended the University of Cambridge, where he studied under renowned intelligence scholars and practitioners to include: Professor Christopher Andrew and Sir Richard Dearlove. His research interests include: improving intelligence analysis, Latin American politics, drug trafficking organizations, anarchist groups, social unrest, and terrorism.

Gregory Treverton stepped down in January 2017 as Chair of the National Intelligence Council, which is the main provider of both strategic intelligence and more immediate intelligence support to senior foreign policymakers in the U.S. government. Earlier, he directed the RAND Corporation's Center for Global Risk and Security, and before that its Intelligence Policy Center and its International Security and Defense Policy Center, and he was associate dean of the Pardee RAND Graduate School. He has served earlier in government for the first Senate Select Committee on Intelligence, handling Europe for the National Security Council and as vice chair of the National Intelligence Council, overseeing the writing of America's National Intelligence Estimates (NIEs). He holds an A. B. summa cum laude from PrincetonUniversity and an M.P.P (Master's in Public Policy) and Ph.D. in economics and politics from Harvard. His latest books are Dividing Divided States, University of Pennsylvania Press, 2014; and Beyond the Great Divide: Relevance and Uncertainty in National Intelligence and Science for Policy, (with Wilhelm Agrell), Oxford University Press, 2015. He is a member of the Council on Foreign Relations and of the Swedish Royal Academy of War Sciences.

Arno H.P. Reuser founded, designed and developed the Dutch Open Source Intelligence Branch (OSINT) and was its manager for more than 20 years. In that time, he designed a revolutionary approach to OSINT for which he was awarded a Platinum Life Time Award. In 2008 he founded Reuser's Information Services devoted to international OSINT consultancy, OSINT training, research, workshops and lectures. In 2013 Arno resigned from the service to work full-time for his company.
Today Arno writes, speaks, reviews, teaches at universities and think tanks worldwide, publishes articles on information topics, runs international training programs and workshops for government and private sector on Open Source Intelligence, writes programmes, gives advice. He runs the

Internet Resource Discovery Toolkit (rr.reuser.biz) and is also a moderator for an information professional discussion list. An interview with Arno can be heard at the International Spy museum in Washington D.C. The latest interview with Arno can be found in eForenics Magazine (http://bit.ly/2dgAGWC). Arno currently lives and works in Leiden, The Netherlands.

Jorhena Thomas is currently a Lecturer in the Applied Intelligence Master's Program at Georgetown University in Washington, DC. She has extensive experience in intelligence analysis, homeland security, and public safety at the international, national, and local levels. Jorhena has also served as Principal Consultant at Wright Thomas International; Chief of Staff to the District of Columbia Deputy Mayor for Public Safety and Justice; Deputy Director at the Washington Regional Threat Analysis Center (the District of Columbia's Intelligence Fusion Center); and Senior Intelligence Analyst with the FBI.

Humberto Hinestrosa is an independent defence and security consultant with experience in the public and private sector. He worked for the Venezuelan intelligence services, as well as various private security providers in Latin-America, IHS-Jane's, and most recently for the International Criminal Court (ICC). His research has been mainly focused on the contributions and challenges of Structured Analytic Techniques (SATs) and more specifically, Scenario Building for intelligence analysis.

Aleksandra Bielska is an educator, analyst and consultant specialising in the collection, analysis and management of intelligence. As an educator, she has taught intelligence theory and practice to public and private sector organisations, including at the NATO's Centre of Excellence in the Defence Against Terrorism in Ankara, Turkey, and the NATO School in Oberammergau, Germany. Her experience covers the entire range of intelligence disciplines including data collection, information and knowledge management, and strategic foresight.

Chris Pallaris is Director and Principal Consultant of i-intelligence. He has over 15 years of experience as an analyst and 10 as a teacher. In addition to his client engagements, he is an Associate Lecturer at Mercyhurst University's Institute for Intelligence Studies. He also teaches courses in the domain of strategic intelligence and knowledge management at the ZHAW's School of Management and Law, and ETH Zurich.

Juan Carlos Ladines Azalia is Professor at Academic Department of Management and Coordinator of the Social Projection Course at the Department of Social and Political Sciences at Universidad del Pacífico, Peru. He holds a Master's degree in Politics and International Relations from Aberystwyth University (Wales – United Kingdom) and a Bachelor's in Economics from Universidad del Pacífico. He has participated as manager of business plans and business networking coordinator of entrepreneurs. He has served as coordinator of institutional projects related to policy and foreign trade. He has experience in Public Governance by supporting various departments within the Peruvian Ministry of Foreign Affairs. He has also taught in schools as professor of economics and business, as well as part-time professor at various universities in courses related to international politics and economics. Currently, he serves as full-time professor of the International Business major and is conducting researches on the field of theories of international relations and business.

William Castillo Stein is a Research Assistant, Academic Department of Management at Universidad del Pacífico. He is also undergraduate student of International Business at Universidad del Pacífico. His interest areas include International Relations, International Business Planning, Emerging Economies, and Political Risk.

Constant Hijzen is an Assistant Professor in Intelligence Studies at the Institute of Security and Global Affairs and the Institute for History at Leiden University (the Netherlands). In his dissertation, he focussed on the political, bureaucratic, and societal context of the Dutch security services. His postdoctoral research focuses on the formative years of intelligence and security services, analyzing their early institutionalization years from a comparative and intelligence culture perspective.

Avner Barnea, Ph.D. is a senior competitive intelligence strategic consultant, teaching strategic CI in various MBA programs in the academia in Israel. He is the head of the special program on competitive intelligence, corporate security, cyber security and crisis management in the MBA program at Netanya Academic College, in Netanya, Israel. Dr. Barnea is also a former senior officer with the Israeli Intelligence Community and currently chairman ofthe Israel CI Forum (FIMAT) and member of SCIP Board of Directors. He is a research fellow, National Security Studies Center, University of Haifa, Israel.

Olivier Chopin is associate-researcher at the École des hautes études en sciences sociales (CESPRA-EHESS) and adjunct senior lecturer at Sciences Po in Paris. His works include Etudier le renseignement, état de l'art et perspectives de recherche he edited for the French ministry of Defense (Études de l'IRSEM n°9, 2012), Pourquoi l'Amerique nous espionne ? (Hikari e, 2014), and most recently Renseignement et Sécurité, a textbook on intelligence written with Benjamin Oudet (Armand Colin, 2016).

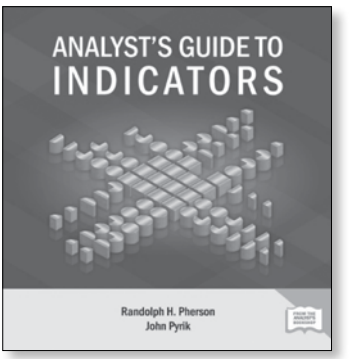
Benjamin Oudet is a PhD candidate in Political Science at the University of Poitiers (France). His research topic is international intelligence cooperation in Europe in the context of counter-terrorism policies and United Nations peacekeeping interventions. He teaches the course: "Shaken and Stirred: Strategic Intelligence in a Changing World" with Olivier Chopin. Sciences Po Paris (France).

Ammar El Benni is a PhD candidate at the "Mihai Viteazul" National Intelligence Academy", Romania. He works as a Romanian Parliament Senior Policy Advisor.

Book Review

Increasing accuracy through more objectivity

Daniela Bacheș-Torres
Efren R. Torres-Bacheș



Randolph H. Pherson, John Pyrik: Analyst's Guide to Indicators

Pherson Associates, LLC, 2017, 96p., $18.95

Analysis objectivity represents a shared concern of both intelligence practitioners and scholars across fields of study and communities of practice. The Office of the Director of National Intelligence (ODNI) acknowledges the importance of analytic objectivity in providing decision makers with relevant and actionable Intelligence on national security issues and events[1]. Likewise, in scientific research, objectivity represents a value as the objective representation of facts and events correspond to capturing a feature of the world[2]. Pherson and Pyrik provide an important working instrument for the broader community of analysts (from various sectors: Intelligence Community, business sector, law enforcement), and fills a gap in the intelligence literature and the social sciences methodology in the *Analyst's Guide to Indicators.*

In the 1st Chapter, Pherson and Pyrik make a presentation of what indicators are, their type (evaluative, estimative and warning indicators), and their role in increasing analysis accuracy. To achieve their pedagogical goal, as well as showcase both their strengths and limits, the two authors use various case studies in which indicators were used. The 2nd Chapter develops the statement made in the first pages about the need to adapt indicators according to the typology and characteristics of the analyzed event. Thus, generating indicators is an analytic process in itself. "[D]epending on the time available, the need for accuracy, and the availability of collection resources (…) [it] can range from simply jotting down things one would expect to see to engaging in sophisticated team effort" (p. 17) that includes using Structured Analytic Techniques (SATs). But even so, the use of indicators does not lack the risk of misunderstanding or misuse which can lead to intelligence or

analytic failures. For this reason, validating indicators (Chapter 3) and clustering them (Chapter 4) represent permanent requirements for analysts throughout their work.

The last two Chapters (5 & 6) are presenting the use of indicators as a tool of the analytic tradecraft in various fields, and are trying to provide examples of the way in which indicators can be used throughout the analytic process of eliminating or reducing the unknown, as well as solving puzzles. The reader will also benefit from the authors' advice on some of the best SATs for generating, evaluating and clustering indicators included in the thirteen Appendices that close the book.

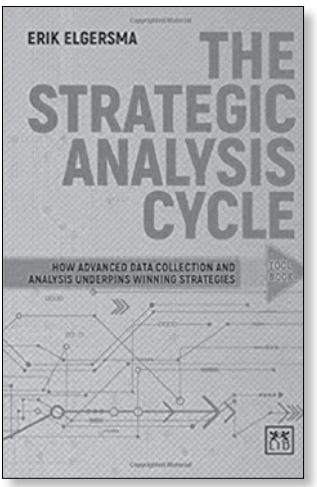
Throughout Pherson and Pyrik's *Guide*, indicators are presented in their twofold role: both as analytic tools, and products of an analytic process. As the authors state in the *Preface*, the book reflects their experience achieved over several decades as analysts, instructors, managers and mentors. Although the *Guide* would have benefited from more theorisation and a more in-depth presentation of how indicators are generated as an independent process, the value of this work resides mainly in the awareness they raise about the general value of this analytic tool. Indicators are a clear example of a tool that crosses domains and sectors of activity, being used by "analysts in intelligence, law enforcement, security, financial, and business sectors".

Endnotes:

*01_* *Intelligence Community Directive (ICD) 203, Analytic Standards*. ODNI, 2015. Available at https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

*02_* Reiss, Julian and Sprenger, Jan, "Scientific Objectivity", *The Stanford Encyclopedia of Philosophy* (Winter 2017 Edition), Edward N. Zalta (ed.). Available at https://plato.stanford.edu/entries/scientific-objectivity/ .

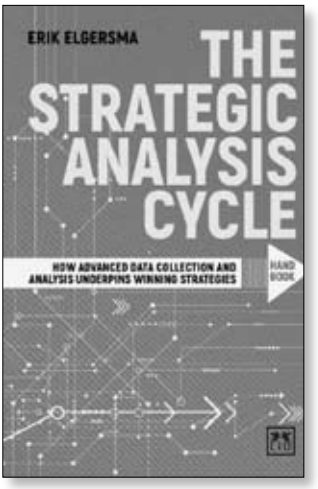
Other 2017 Publications on Intelligence Analysis



Erik Elgersma

The Strategic Analysis Cycle Tool Book: How Advanced Data Collection and Analysis Underpins Winning Strategies

LID Publishing, 2017, 288p., $20.81



Erik Elgersma

The Strategic Analysis Cycle Hand Book: How Advanced Data Collection and Analysis Underpins Winning Strategies

LID Publishing, 2017, 400p., $29.19

Mark Lawrence Ashwell, (2017)

"The digital transformation of intelligence analysis"

Journal of Financial Crime

Vol. 24 Issue: 3, pp.393-411, https://doi.org/10.1108/JFC-03-2017-0020

JOURNAL *of* MEDITERRANEAN *and* BALKAN INTELLIGENCE
AN INTERNATIONAL JOURNAL

Instructions for Authors

Submission of Manuscripts. Manuscripts should be submitted electronically in Microsoft Word (doc or docx) to the **Editor, Dr. John M Nomikos, Research Institute for European and American Studies, *secretary@rieas.gr*** Each manuscript must be accompanied by a statement that it has not been published simultaneously for publication elsewhere. As an author, you are required to secure permission if you want to reproduce any figure, table, or extract from the text of another source. All accepted manuscripts, artwork, and photographs become the property of the Publisher. **Manuscripts must be maximum 8.000 words and Abstracts must be around 400 words.** All manuscripts including title page, abstracts, tables, and legends, should be typewritten, ***one and half spaced (1 & 1/5).*** All margins should be at least one inch and all pages should be numbered consecutively throughout the manuscript. Titles must be as brief and clear as possible. **All references should be numbered consecutively at the end of the paper (Endnotes).** In the text, references should be cited by a superior character of the corresponding number. For further information, consult The Chicago Manual of Style, 14th edition. All articles undergo a rigorous double-blind peer review process.

Affiliation

On the title page, include full names of authors, academic/or other professional affiliations, and the complete mailing address of the author to whom proofs and correspondence should be sent.

Tables and Figures

Tables and figures should not be embedded in the text, but should be included as separate files. A short descriptive title should appear above each table with a clear legend and any footnotes suitably identified below. All units must be included. Figures should be completely labeled, taking into account necessary size reduction. Captions should be typed, one and half spaced, on a separate sheet.

Proofs

All proofs must be corrected and returned to the Editor. If the proofs are not returned within the allotted time, the Editor will proofread the article and it will be printed per editor's instructions. Only correction of typographical errors is permitted. When the journal is published, authors will receive two copies of the Journal for Mediterranean and Balkan Intelligence (JMBI).

ISSN 2241-4991