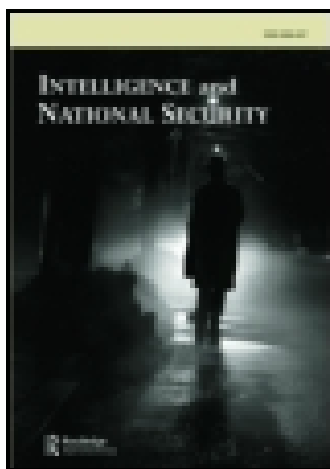


This article was downloaded by: [University of Central Florida]

On: 06 June 2015, At: 08:55

Publisher: Routledge

Informa Ltd Registered in England and Wales Registered Number: 1072954 Registered office: Mortimer House, 37-41 Mortimer Street, London W1T 3JH, UK



Intelligence and National Security

Publication details, including instructions for authors and subscription information:

<http://www.tandfonline.com/loi/fint20>

Spies and Policymakers: Intelligence in the Information Age

Marcos Degaut

Published online: 19 Mar 2015.



CrossMark

[Click for updates](#)

To cite this article: Marcos Degaut (2015): Spies and Policymakers: Intelligence in the Information Age, *Intelligence and National Security*, DOI: [10.1080/02684527.2015.1017931](https://doi.org/10.1080/02684527.2015.1017931)

To link to this article: <http://dx.doi.org/10.1080/02684527.2015.1017931>

PLEASE SCROLL DOWN FOR ARTICLE

Taylor & Francis makes every effort to ensure the accuracy of all the information (the "Content") contained in the publications on our platform. However, Taylor & Francis, our agents, and our licensors make no representations or warranties whatsoever as to the accuracy, completeness, or suitability for any purpose of the Content. Any opinions and views expressed in this publication are the opinions and views of the authors, and are not the views of or endorsed by Taylor & Francis. The accuracy of the Content should not be relied upon and should be independently verified with primary sources of information. Taylor and Francis shall not be liable for any losses, actions, claims, proceedings, demands, costs, expenses, damages, and other liabilities whatsoever or howsoever caused arising directly or indirectly in connection with, in relation to or arising out of the use of the Content.

This article may be used for research, teaching, and private study purposes. Any substantial or systematic reproduction, redistribution, reselling, loan, sub-licensing, systematic supply, or distribution in any form to anyone is expressly forbidden. Terms &

ARTICLE

Spies and Policymakers: Intelligence in the Information Age

MARCOS DEGAUT*

ABSTRACT Massive changes and continuous developments in the uses and applications of technology and communications have changed the way we see the world. The Information Revolution has had an impact upon intelligence collection, processing, analysis, and dissemination, and upon the way policymakers can access reliable information, in a timely manner, and upon the sources they are most likely to rely on when a specific piece of information is needed to support a decision. This study attempts to describe, analyze and explain the nature of the ongoing Information Revolution, to present its main impacts on the intelligence and policy communities, to discuss the relationship between the Intelligence Community and policymakers, and to propose what the IC should do to meet the high expectations of decision-makers.

Introduction

One of the most pressing challenges faced by the Intelligence Community (IC) nowadays concerns how to deal with the effects of the massive changes and continuous developments in the uses and applications of information and communications technologies (ICTs) – part of the process known as Information Revolution (IR) – upon intelligence collection, processing, analysis, and dissemination. The development and increasing interconnect-edness of ICTs such as the internet, satellite television, and mobile phones,¹ along with the widespread use of social communication networks such as Facebook and Twitter have helped reshape every aspect of political, economic, social, and cultural life, changing the way we see the world.²

The IR has transformed the world's most advanced nations from industrial to information-based societies, creating new opportunities for those who

*Email: marcosdegaut@knights.ucf.edu

¹Johan Eriksson and Giampiero Giacomello, 'The Information Revolution, Security, and International Relations: (IR)relevant Theory?', *International Political Science Review* 27/3 (2006) pp.221–44.

²Onook Oh, Manish Agrawal and Raghav Rao, 'Community Intelligence and Social Media Services: A Rumor Theoretic Analysis of Tweets during Social Crises', *MIS Quarterly* 37/2 (2013) pp.407–26.

understand its nature and master its principles and tools. It has brought economic development, improved person-to-person contact and understanding, and revolutionized other areas of human interaction, such as politics, education, entertainment, and trade, among many others. Copeland, for instance, notes that the US military seeks to explore multiple ways to seize information superiority during conflicts and thus gain decisive advantages over its opponents.³ On the other hand, advances and improvements in ICTs have introduced new challenges and threats to intelligence services, by enabling governments, criminal organizations, terrorist groups, and individuals with malign or subversive intentions to conduct new kinds of activities contrary to national interests and the global security.⁴ As a consequence of this 'new' threat environment, characterized by accelerating change, increasing complexity and rising uncertainty, official agents, structures, and institutions responsible for providing information and *foreknowledge* to decision-makers have been 'tasked with monitoring threats to their country's national security interests that are more diverse, interconnected and dynamic than ever before',⁵ which has made their job significantly more difficult.

Likewise, the IR has had a deep impact upon the traditional intelligence cycle, affecting the way policymakers can access reliable information, in a timely manner, and the sources they are most likely to rely on when a specific piece of information is needed to support a decision. It has not only affected the relationship between the IC and decision-makers, but has also created an apparent tension between official intelligence structures and the open source information provided by the 'business intelligence' industry. Until not long ago, decision-makers were almost entirely dependent on the information and intelligence reports provided by the IC.⁶ To some extent, the IR has changed that scenario by allowing individuals to obtain an unbelievable amount of information – that will not necessarily be turned into knowledge – from a multitude of sources, which has arguably resulted in a more informed and independent policymaker.⁷

Nowadays, it seems that the IC has to compete for policymakers' attention with media and other information brokers who communicate and disseminate information on global events instantaneously through ICTs, like the terrorist attacks in Mumbai, in November 2008, the Iran post-

³Thomas Copeland (ed.), *The Information Revolution and National Security* (Carlisle, PA: Strategic Studies Institute, US Army War College 2000).

⁴Peter Bell and Mitchell Congram, 'Communication Interception Technology and its Use in the Fight against Transnational Organised Crime in Australia: A Review of the Literature', *The International Journal of Social Science Research* 2/1 (2014) pp.46–66.

⁵Myriam Dunn Cavelty and Victor Mauer, 'Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence', *Security Dialogue* 40/2 (2009) pp.123–44.

⁶John Coyne, Stuart Neal and Peter Bell, 'Reframing Intelligence: Challenging the Cold War Intelligence Doctrine in the Information Age', *International Journal of Business and Commerce* 3/5 (2014) pp.53–68.

⁷Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (London: Sage Press 2012).

election demonstrations in June 2009, the 11 September 2012 attacks on the US Special Mission (and a nearby CIA annex) in Benghazi, Libya, as well as the Arab Spring ‘social media’ revolution, episodes in which Facebook, Flickr, and Twitter, among other social networks, were massively used to diffuse news. Non-intelligence sources of analysis have become so advanced, broadcasting information in real time via the Internet, cell phones, or satellite feed to constantly reporting news services, for example, that some policymakers may have found intelligence might be losing part of its competitive advantage. Some scholars argue that intelligence clients have already begun to ‘question the “value” of intelligence capabilities when so much other information is available, especially users who have found intelligence slow, inconclusive, or hidebound by classification rules and other controls’.⁸

Confronted on a daily basis by the challenges imposed by the IR, intelligence officers, policymakers, and scholars must first understand the nature of this revolution and the effects it potentially has on policy and intelligence communities, if they also want to change, reform, and adapt to the information age. It might turn out that, far from being relegated to a secondary position, the IC could have its value reinforced. Due to the avalanche of information available, policymakers will likely demand the IC to provide more relevant and timely assessments with knowledgeable insight into the capabilities, intentions, ideologies, motivations, activities, and trends related to individuals, groups, and organizations that might pose a threat to national security and interests. In that case, the IC will have to work harder not only to collect information that other actors want to keep secret, but also to compile, process, analyze, and validate myriad threads of information obtained from non-intelligence sources, ‘promptly and in a manner that would permit them to take timely decisions to head off or influence events that might adversely affect US interests’.⁹

This study aims to discuss the main impacts of the IR on intelligence and policy communities, the relationship between these actors in the information age, and what the IC is expected to do to meet the heightened expectations of policymakers, in order to preserve its vital role in the decision-making process. The paper proceeds as follow. The first section describes and analyzes the nature of the IR. It then identifies the impacts of the IR upon the IC and the intelligence cycle, focusing on the apparent tension between the IC’s traditional role and the services provided by private information brokers. This section also analyzes how social networking platforms can be not only an invaluable channel of information acquisition, but also a threat to national security. Finally, this paper discusses how the IR affects the IC’s relationship with the policymaking community.

⁸Deborah Barger, *Toward a Revolution in Intelligence Affairs* (Santa Monica, CA: Rand Corporation 2005).

⁹Intelligence and National Security Alliance (INSA), *Expectations of Intelligence in the Information Age*, 2012.

The Information Revolution

The IR is a phenomenon that defies simple characterization, being heralded as ‘the greatest global transition since the Industrial Revolution’.¹⁰ Rosenau suggests that the IR, ‘by providing technologies that have continued to greatly accelerate the collapse of time and space, has added substantially to the complexities that mark our time’.¹¹ Maniscalco sustains that, in consequence, the relevance of distance and time in individuals and populations’ lives has been dissolved.¹² In fact, Williams, Dunlevy and Shimeal observed that less than 10 years ago the development of ICTs had become a critical component of globalization, shrinking both time and space: ‘with far-reaching consequences that are still barely understood. Hi-tech connectivity has facilitated the emergence of dense global commercial and information networks that are unprecedented in their speed, accessibility, and capability’.¹³

For operational purposes, the IR can be understood as the ‘ongoing social, political, and economic change brought about by technological advances in computing and telecommunications’.¹⁴ Its defining trait is the increasing networking of computers,¹⁵ which is the first true many-to-many communications medium. When the complementary technologies of computers and telecommunications are integrated to create networks of interconnectivity, whose most remarkable result is the internet, opportunities for new applications and utilities proliferate.¹⁶ The exponential growth in both the power of this technology and its widespread use, since it is used by almost 4.3 billion people around the world,¹⁷ associated with its dramatically reduced costs, is what has allowed the current period to be termed a ‘revolution’. Its main product is information itself, which is expanding and spreading at an unprecedented rate, providing the individual with an ever expanding quantity and variety of information. The indexed World Wide Web (WWW) reached over 4.39 billion pages on 23 December 2014.¹⁸ The natural consequence of the dissemination of this technology is the proliferation of information consumers and providers.

¹⁰Copeland, *The Information Revolution*, p.1.

¹¹James Rosenau, ‘The Information Revolution: Both Powerful and Neutral’ in Copeland, *The Information Revolution*, pp.9–29.

¹²Luisa Maria Maniscalco, ‘Living in the Cyber Era: Reflections on Security in a Hybrid World’, Mediterranean Council for Intelligence Studies Yearbook 2012, pp.13–8.

¹³Phil Williams, Casey Dunlevy and Tim Shimeal, ‘Intelligence Analysis for Internet Security’, *Contemporary Security Policy* 3/2 (2010) pp.1–38, p.1.

¹⁴Lorne Teitelbaun, *The Impact of the Information Revolution on Policymakers’ Use of Intelligence Analysis* (Santa Monica, CA: Rand Corporation 2004) p.80.

¹⁵Jim Dewar, *The Information Age And The Printing Press: Located Backward to See Ahead* (Santa Monica, CA: Rand Corporation 1998).

¹⁶Teitelbaun, *The Impact of the Information Revolution*.

¹⁷ < <http://www.factsshunt.com/2014/01/world-wide-internet-usage-facts-and.html> >

¹⁸ < Worldwidewebsite.com >

Today, for example, journalists, protesters, online commentators – known as bloggers – and political activists anywhere in the world can report ongoing events in real time, broadcasting their report directly to the internet, and provide streaming full-motion video with analysis. One law-enforcement officer once dramatically complained: ‘I believe we should get more information – before news media does. It seems police are the last to know and the first to get a call!’¹⁹ Other information suppliers using the WWW can distribute the latest information from databases and other information repositories as events take place, or in immediate response to most information requests, which contributes to affect the content of media coverage and to shape political events across the world. Everyday millions of bloggers share their opinions on domestic and international events with an increasingly wider audience. Only one of the most popular political blog, *The Huffington Post*, is reported to have over 110 million visitors.²⁰ Among the most influential political blogs, some belong to the main stream media, such as the CNN’s *Fareed Zakaria*, while others are well-know partisan bloggers, like the liberal Center for American Progress’ *Think Progress*, the conservative National Review’s *The Corner*,²¹ and the American Conservative’s *Daniel Larison*. The top five political blogs alone were reported to attract over half a million visitors per day.²² These influential blogs have become aggregators of information and analysis, allowing decision-makers to extract meaningful insights and to use these sources to ‘help them interpret and predict political developments’.²³ Although the media and other information suppliers may not necessarily influence policymakers directly, they can do so via public opinion by shaping people’s perceptions, knowledge, and beliefs about foreign politics. In that regard, Kingdon has found in a study on the media’s role on policymaking that governments tend to pay more attention to issues that are more extensively covered by the media, basing their decisions on what they believe to be the ‘mood of the nation’.²⁴

In fact, the IR is transforming industrial societies into information-based societies. In a context where ‘[p]ieces of data have become the building blocks of many modes of human interaction and activity’,²⁵ what makes these changes worthy of being considered a real revolution is ‘their degree of social penetration that makes our society a “network society” [...] which revolves around the innovations dictated by technological developments’.²⁶

¹⁹Barger, *Toward a Revolution in Intelligence Affairs*, pp.20–1.

²⁰< <http://www.ebizmba.com/articles/political-websites>>

²¹Nitya, ‘Who is Who in the Political Blogosphere’. *ABC News*, 3 June 2009 <<http://abcnews.go.com/blogs/politics/2009/06/whos-who-in-the-political-blogosphere/>>

²²Daniel W. Drezner and Henry Farrell, ‘Web of Influence’, *Foreign Policy*, 26 October 2009 <<http://foreignpolicy.com/2009/10/26/web-of-influence/>>

²³*Ibid.*

²⁴John Kingdon, *Agendas, Alternatives and Public Policies* (Upper Saddle River, NJ: Longman 2011).

²⁵Copeland, *The Information Revolution*, p.2.

²⁶Maniscalco, ‘Living in the Cyber Era’, p.13.

Governments, international institutions, private companies, and individuals rely increasingly on high-speed and high-quality information to conduct their daily functions and operations. The development of advanced ICTs has not only facilitated the exercise of *soft power* but has also made clear that military capabilities today are increasingly dependent on them, as recent American military operations and the extensive use of unmanned aerial vehicles to search insurgents in Iraq and Afghanistan have proven. What seems to be a ‘doctrinal and organizational change in the way of waging war’,²⁷ known as Revolution in Military Affairs (RMA), has led the United States to place an ever-growing emphasis on electronic management of information to ensure national security. Likewise, electronic attacks directed towards the critical infrastructures and communications networks of states have proven to be a real danger to the security of information-dependent societies,²⁸ as the 2008 Russian armed attack against Georgia, accompanied by cyber attacks that crippled Georgia’s military and public systems, can illustrate.

The Information Revolution’s Impacts on Intelligence: The New Information Environment

The IR has had impacts upon every bureaucratic institution, and the IC could not escape this reality. It has changed the way the IC works and has influenced how policymakers perceive and use intelligence. To Liaropoulos:²⁹ ‘the Information Revolution affects every step of the intelligence cycle; it adds new issues in the intelligence agenda, alters old ones and brings profound organizational and cultural changes in the art of intelligence’. It also has changed the way international and security-related events take place and the way policymakers are supposed to react to those events, altering the way intelligence consumers interact with information. Whether or not this is accepted in the IC, the IR has to some extent changed how policymakers access information, as well as the sources they can rely on to support foreign policy decisions. As a retired senior CIA officer stated ‘our customers are smarter and more sophisticated than we give them credit for; they have their own independent sources of information and analysis with which we are competing’.³⁰

A survey conducted by the Senior Executive Intelligence Bureau in 2000 – at a time when ICTs were much less developed than they are now – revealed that 85% of the decision-makers interviewed relied on all four of the

²⁷Ibid., p.17.

²⁸Anthimos Alexandros Tsirigotis, ‘Military Strategy in the Cyber Era: Continuity and Changes’, Mediterranean Council for Intelligence Studies Yearbook 2012, pp.19–27.

²⁹Andrew N. Liaropoulos, A (R)evolution in Intelligence Affairs? In Search of a New Paradigm. Research Institute for European and American Studies, Athens, Greece, Research Paper N. 100, June 2006, p.7.

³⁰Martin Petersen, ‘What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers’, *Studies in Intelligence* 55/1 (2011) pp.13–20, p.15.

following sources to stay more informed about recent events and their developments: foreign newspapers and weekly periodicals, US newspapers and weekly periodicals, their professional networks, and official, informal communications, such as email.³¹ Policymakers nowadays are ‘accustomed to having unrestricted access to globally sourced and indexed information and will be adept at analyzing that data’.³² In this scenario, one of the main challenges facing the intelligence officer is to add value and context to information that the client has most probably already seen,³³ reason why the IC has to establish its ‘credibility and usefulness individual by individual, administration by administration’.³⁴

The new environment under which the IC operates has some very important characteristics, one of which is interactivity. This feature generates unintended consequences from seemingly isolated actions, which are also often unpredictable,³⁵ as ‘what happens in the real world has an immediate repercussion on the web and vice-versa’.³⁶ The WWW connects and brings into contact every country, international organization, major private companies, and other relevant actors in the international system. Through this global information grid, each actor is notified of the other’s actions and possible intentions in an almost instantaneous way, which allows the emergence of a system of interactions too complex to predict. The Arab Spring, which arose in part from the domino effect unleashed by the Tunisian revolt throughout the Maghreb – resulting in the direct overthrow of the governments of Tunisia, Libya, and Egypt, and the destabilization of others, including Syria – is a powerful example of the interactivity and the ‘amplification and speed up of emulation and “contagion” dynamics implemented by web-enabled connections’.³⁷

Perhaps, one of the most important characteristics is speed. Policymakers need to act quickly to respond to specific events as they take place in real time because increased interactivity means changes take place in much shorter time intervals.³⁸ Thus, ‘in an age of instant information generated by individuals with smartphones from the streets of urban centers (as well as distant battlefields), policymakers will want their “current, actionable” intelligence not in days or hours, but in real time’.³⁹ Speed affects all other

³¹Carmen Medina, ‘What to Do When Traditional Models Fail?’, *Studies in Intelligence* 46/3 (2002) pp.23–9.

³²INSA, *Expectations of Intelligence in the Information Age*, p.7.

³³Magdalena Duvenage, *Intelligence Analysis in the Knowledge Age: An Analysis of the Challenges facing the Practice of Intelligence Analysis* (Stellenbosch: Stellenbosch University 2010) p.35.

³⁴Petersen, ‘What I Learned in 40 Years’, p.15.

³⁵Richard Burt and Olin Robison, *Reinventing Diplomacy in the Information Age*. Center for Science and International Studies (CSIS), 1998.

³⁶Maniscalco, ‘Living in the Cyber Era’, p.13.

³⁷*Ibid.*, p.14.

³⁸Johanna Neuman. *Lights, Camera, War: Is Media Technology Driving International Politics?* (NY: St. Martin’s Press 1996).

³⁹INSA, *Expectations of Intelligence in the Information Age*, p.6.

features and is a multiplier of interactivity, because the virtually real-time communications of the IR only increase its impact. The media is to some extent able to drive the policymaking process by delivering information to a global audience and making a big enough impact on the populace that they demand action from their government.⁴⁰

The third characteristic is the proliferation of *new actors* and *unfamiliar actors*.⁴¹ The state is not the only relevant actor in International Relations anymore. International business, NGOs, multilateral institutions, think-tanks, terrorist and interest groups, and criminal organizations, among others, are also powerful actors in foreign affairs, which mean that foreign governments are hardly the only source of threat to national security and interests. More actors add more complexity to the international order and increase even further the level of uncertainty.⁴² Additionally, this situation puts a premium on the need for the IC to further develop its 'social intelligence' capabilities, especially when one considers that many relevant information circulate firstly on social media networks and the internet, and only later are echoed by the mainstream media and other information suppliers. At the height of the mass protests that followed the June 2009 presidential election in Iran, for example, Twitter was the most important communication platform used by journalists and demonstrators to stream happenings to the world, due to the Iranian authorities' media blackout, bringing the 'violence in the streets of Tehran to the forefront of the geopolitical conversation'.⁴³ Considering that nowadays over 80% of all internet users regularly utilize social media networks,⁴⁴ most of them on a daily basis, its advent has not only created an environment of greater interactivity among organizations, businesses, and people,⁴⁵ but has also changed the way people create, distribute, and share information, especially during political or social crises.⁴⁶

It is no wonder then that open-source information gathered from online social media form the 'geopolitical backdrop to what may be seen as the new cutting edge in open-source tactical intelligence collection'.⁴⁷ Social media sites have become 'the gold mine of intelligence',⁴⁸ invaluable sources of information acquisition for intelligence and law enforcement entities. The US

⁴⁰Burt and Robison, *Reinventing Diplomacy in the Information Age*.

⁴¹Teitelbaun, *The Impact of the Information Revolution*.

⁴²Cavelty and Mauer, 'Postmodern Intelligence'.

⁴³Jared Keller, 'Evaluating Iran's Twitter Revolution', *The Atlantic*, 18 June 2010 <www.theatlantic.com/technology/archive/2010/06/evaluating-irans-twitter-revolution/58337/>

⁴⁴Joseph Fitsanakis and Micah-Sage Bolden, 'Social Networking as a Paradigm Shift in Tactical Intelligence Collection', *Mediterranean Council for Intelligence Studies Yearbook* 2012, pp.28–40.

⁴⁵Global Advisory Committee, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities*, US Attorney General, 2013.

⁴⁶Oh, Agrawal and Rao, 'Community Intelligence and Social Media Services'.

⁴⁷Fitsanakis and Bolden, 'Social Networking as a Paradigm Shift', p.28.

⁴⁸Stilgherrian, 'Has Facebook Killed the Undercover Cop?', CSO, 25 August 2011 <http://www.cso.com.au/article/398581/has_facebook_killed_undercover_cop/>

Department of Defense already considers online social media as ‘both a resource and a weapon in future conflicts’⁴⁹ and is investing heavily to develop its social media collection capabilities, including methods to follow and shape events, and to ‘proactively influence internet conversations and spread pro-American propaganda’.⁵⁰ However, criminals, terrorists, and potentially dangerous individuals and organizations are also using these networks with malign intents. These platforms are increasingly being used for a wide range of possibilities which include the instigation, coordination, or conduction of criminal activities, cyber terrorist attacks, and the dissemination of subversive ideologies. Terrorist groups, such as the Islamic State (IS), have been undertaking sophisticated campaigns through social media networks not only to disseminate their criminal intentions and activities, to foster sympathy for their cause, to expand the reach of their propaganda, to plan and coordinate their attacks across the world, to communicate with their supporters and ethnic diasporas, to solicit donations, and to recruit and train new members,⁵¹ addressing them towards the theatres of conflict, but also to create off-shoot organizations in new areas.⁵² Consequently, intelligence officers must understand how social media sites work, which tools and resources are made available to them, and how they can speed up the development of collection protocols, methods, and techniques to monitor, prevent, mitigate, and respond to threats to national security, in a context where ‘[f]inding a way to close the validation cycle on social intelligence and melding it with traditional intelligence will be a demand the IC can expect from policymakers’.⁵³

The fourth trait is *feedback*, which results from the flow of relevant and accurate information delivered to policymakers through traditional transmission channels and through information age channels as well. To Burt and Robison,⁵⁴ policymakers have traditionally used public opinion polls and other mechanisms to ‘gauge the positions of constituents, foreign governments and international actors, but the explosion of information conduits could conceivably give every affected actor or agency a venue for sending feedback to policymakers about any specific policy or decision’.

Despite the importance of these features, a potential source of confusion for both the IC and policymakers is that as much as the external environment has increased in complexity, the internal policymaking environment in some cases has not changed at all from the way it collected, processed, and filtered

⁴⁹David Streitfeld, ‘Pentagon Seeks a Few Good Social Workers’, *The New York Times*, 2 August 2011 <<http://bits.blogs.nytimes.com/2011/08/02/pentagon-seeks-social-networking-experts/>>.

⁵⁰Fitsanakis and Bolden, ‘Social Networking as a Paradigm Shift’, p.34.

⁵¹Gabriel Weimann, ‘Terrorist Facebook: Terrorists and Online Social Networking’, in M. Last and A. Kandel (eds.) *Web Intelligence and Security* (Amsterdam: IOS Press 2010) pp.19–29.

⁵²Shaul Shay, ‘Al Qaeda and the Hybrid Jihad’, in M. Last and A. Kandel (eds.) *Web Intelligence and Security* (Amsterdam: IOS Press 2010) pp.31–5.

⁵³INSA, *Expectations of Intelligence in the Information Age*, p.8.

⁵⁴Burt and Robison, *Reinventing Diplomacy in the Information Age*, p.31.

information prior to the information age. Cavelty and Mauer⁵⁵ contend that the doctrine, organizational structures, and decision-making mechanisms of the IC appear to have stagnated in the post-Cold War period, perhaps because the essence of the role of the intelligence professional has changed very little since the beginning of the Cold War.⁵⁶ Likewise, Coyne, Neal and Bell argue that ‘very little appears to have changed with regards to the analytical tradecraft at this time. One of the fundamental questions for the intelligence profession is to determine if its half century old intelligence doctrine remains valid and reliable today’.⁵⁷ It thus now imperative that the IC understand how these external interactions operate because, to some extent, intelligence analysts now find themselves in competition with new information sources for policymakers’ attention, who are likely to expect the IC to outperform private information brokers, in a context where, with more issues, more actors, and more government and cross-sectoral consumers, ‘all stimulated by the notion that in the new information environment, information carries a premium for effective behavior’,⁵⁸ there is a demand boom for intelligence products.

Therefore, if the methods and technology used by the IC, for example, to collect, analyze, and disseminate intelligence are, as some would argue, obsolete (not proven so far), the ability to inform policymakers becomes seriously damaged. Ignoring modern technology denies policymakers the potential benefits of the analytic, search, communications, and networking tools that might be available. At the same time, however, technological solutions are systematically being pursued by the private sector in order to exploit opportunities made possible by the IR. Some believe that access to open sources through new information technologies arguably levels the playing field in intelligence collection between public and private entities. Policymakers have to understand the nature of these interactions between information sellers and information consumers in order to get the best possible support.

Not long ago, it was assumed that both the information and the technology provided by intelligence agencies were more relevant than that provided by other sources. That assumption has been severely challenged and might not be entirely accurate anymore. To some extent, the idea that the IC had a certain monopoly on the elements of a quality intelligence product is becoming less and less credible. The IC, which historically enjoyed a leadership position in supplying policymakers with information and knowledge, must now compete against new and sophisticated suppliers of data and analysis. Some scholars argue that the private sector might not only be able to provide more relevant information in a more timely manner to

⁵⁵Cavelty and Mauer, ‘Postmodern Intelligence’.

⁵⁶Peter Gill, Stephen Marrin and Mark Phythian (eds.), *Intelligence Theory: Key Questions and Debates* (NY: Routledge 2009) pp.208–26.

⁵⁷Coyne, Neal and Bell, ‘Reframing Intelligence’, p.53.

⁵⁸Davis Bobrow, ‘Exploiting Open Source Information’, in Copeland, *The Information Revolution*.

consumer, but it could also develop products and services and provide technologies that might best fits customer's needs. The Intelligence and National Security Alliance observes that the 'sources, methods, tools, and products available in the private sector rival and, in many instances, surpass those of the IC',⁵⁹ while Coyne, Neal and Bell⁶⁰ contend that the IR:

[...] has arguably displaced the unquestioned pre-eminence of intelligence in public sector decision-making. In the post-modern information age, it has become far less clear to the policymaker or decision-maker what intelligence is and what unique service or product it provides. The cold war era doctrine of intelligence theory is underpinned by a construction of the client as an entity unable to access or assess data and information. In this context, intelligence is at best, a classified information source.

In this new scenario, the IC must understand that it is in an extraordinarily competitive environment, made up of a complex group of domestic and foreign processors, collectors, analysts who are competing for business, and consumers. Supplying information in the information age requires the ability to deliver data and analysis to consumers from the widest possible selection of sources almost instantaneously, and very often in real time as events take place, which means that these competitors have to systematically improve their services, products, and the quality of information they deliver. As the accessibility to information becomes ubiquitous, the competition for 'markets' becomes harder. Providers able to continuously innovate and to add 'value' and 'context' to their information are more likely to have larger shares of this market, while those who fail to keep up or who lag behind tend to be marginalized. If news sources of data and analysis, a large part of which were once denied or mostly restricted to the IC, are now openly and readily available everywhere to everyone, it raises the question of whether the IC has been able to adapt over time to offer support to policymakers in ways that commercial and other non-intelligence sources of analysis cannot. If the IC has not been able to adapt, to perform structural changes, and to compete, and non-intelligence sources have developed methods, tools, and resources to provide more useful information to decision-makers in a more timely way, then the role of the IC begins to be seriously questioned.

Policymakers and the Information Revolution: Their Relationship with the Intelligence Community

To some extent, the IR is making available information that governments and the IC once considered secret intelligence. From Google Earth images of suspected nuclear facilities in Iran to social media feeds' descriptions of Russian troops' deployment along the Ukrainian borders, new and evolving

⁵⁹INSA, *Expectations of Intelligence in the Information Age*, p.9.

⁶⁰Coyne, Neal and Bell, 'Reframing Intelligence', p.58.

sources of information are allowing ordinary people, journalists, businessmen, scholars, and policymakers to obtain insights into issues that, even recently, only intelligence collection could hope to answer. The emergence of this new information environment also led to a major structural change in the policymaking environment, affecting the way decision-makers interact with information and intelligence providers. Liaropoulos⁶¹ summarizes the essence of the impact of the IR on the IC and policymakers: 'In the recent past information was scarce (often the product of clandestine operations), expensive and considered authoritative. On the contrary, information nowadays is relatively accessible, cheap and more tangible'. This means that the ability to systematically observe the world and report the most pressing issues to policymakers is no longer monopolized by the IC (if it ever was). Dupont estimates that nearly 80% of the data held by US intelligence agencies is unclassified, open source information readily available within the public domain.⁶² While some scholars and practitioners tend to attribute more value to covertly obtained information,⁶³ others believe that intelligence can be any information obtained from any source that might contribute to the decision-making process,⁶⁴ forming a scenario in which the IC is expected to make more effective use of open information, converting them into usable information, to keep decision-makers aware of threats and opportunities. Certainly, only traditional intelligence can satisfy some information needs, especially in subjects linked to military, criminal, and diplomatic activities, among others; likewise, there is information the private sector cannot access, due to legal restrictions or the costs and logistics involved, which gives the IC a comparative advantage as it is better situated to collect information that others want to keep secret. However, the existence of secrets still there to be 'stolen' does not mask the fact that the world is now a much smaller, freer, and open place, due to the revolution brought about by advances in ICTs.

Furthermore, the informatics tools needed to manage and disseminate the vast amount of data and information available to decision-makers not only can be found and produced everywhere, but their technical interfaces are also much easier to use and to be mastered. People and open source news organizations can now report from almost anywhere on the planet in real time as events take place, in a relatively free way and inexpensive manner,

⁶¹Liaropoulos, A (R)evolution in Intelligence Affairs?, p.8.

⁶²Alan Dupont, 'Intelligence for the Twenty-First Century', *Intelligence and National Security* 18/4 (2003) pp.15–39.

⁶³Mark Lowenthal, *Intelligence from Secrets to Policy*, 3rd ed. (Washington, DC: CQ Press 2006); Gustavo Diaz-Matey, 'Intelligence Studies at the Dawn of the 21st Century: New Possibilities and Resources for a Recent Topic in International Relations', Madrid, Spain, UNESCO Discussion Papers, N. 8, 2005, pp.1–15.

⁶⁴Gregory Treverton, *Reshaping National Intelligence for an Age of Information* (Cambridge: Cambridge University Press 2002); Michael Warner, 'Intelligence as Risk Shifting', in P. Gill, S. Marrin and M. Pythian (eds.) *Intelligence Theory: Key Questions and Debates* (NY: Routledge 2009) pp.16–33.

blurring much of the need to develop sophisticated intelligence collection systems and networks to find out basic facts about foreign governments and other international actors. At the same time, changes in international politics have made open sources increasingly more important to intelligence consumers. It must be noted that nowadays foreign policy events take place in much shorter time cycles than ever before, as well as our ability to react to them, creating a need for more information, more comprehensive information, and more timely, accurate, and reliable information. However, more information does not mean better intelligence, since, among other problems, it might produce more disinformation and propaganda, or could simply be wrong, as well as access to more information does not necessarily lead to better decision-making or 'situational awareness'.⁶⁵ Mustafaraj and Metaxas have found, for example, that some of Google's real-time search results for Tweeter, news websites, and blogs reveal that real-time information was mostly 'fabricated content, unverified events, lies and misinterpretation'.⁶⁶ Although sharing some common traits with information, intelligence, whether as product, process, or organization, is much more than information. And, without ignoring the convertibility of information into knowledge, information does not turn necessarily into knowledge. Information is data, to which some level of meaning and context was provided, in order to describe a situation or condition⁶⁷; without evaluation and analysis, the collected information may lose its usefulness. Knowledge, on the other hand, is built on data and information and 'represents understanding of the context, insights into the relationships within a system and the ability to identify leverage points and weaknesses and to understand the future implications of actions taken to resolve problems'.⁶⁸

With so much information available, information users can feel frustrated and empowered at the same time. The empowerment results from the ability to undertake a research on any subject or be informed about the latest news on any event without leaving your own home or office. The frustration is a result of the 'information overload' phenomenon, which takes place when users find it difficult to find and assess the validity of specific information they need 'among the ever increasing worldwide storehouse of information and continually proliferating information repositories'.⁶⁹ In this environment, policymakers could continue relying mostly on intelligence analysis, 'but it is

⁶⁵E. Allison Newcomb and Robert J. Hammell II, 'Examining the Effects of the Value of Information on Intelligence Analyst Performance', 2012 Proceedings of the Conference on Information Systems Applied Research, New Orleans, pp.1–10, p.1.

⁶⁶Eni Mustafaraj and Panagiotis Metaxas, 'From Obscurity to Prominence in Minutes: Political Speech and Real-Time Search', Proceedings of the WebSci10: Extending the Frontiers of Society On-Line, Raleigh, NC, 26–27 April 2010, p.1.

⁶⁷Alex Bennet and David Bennet, 'The Rise of the Knowledge Organization', in C. Holsapple (ed.) *Handbook on Knowledge Management Volume 1: Knowledge Matters* (Berlin: Springer 2003) pp.5–21.

⁶⁸Ibid.

⁶⁹Burt and Robison, *Reinventing Diplomacy in the Information Age*, p.13.

unclear if the intelligence community has adapted to the new changes in the environment in which it operates'.⁷⁰

This framework presents two main consequences. First, some scholars argue that the consumer of intelligence products has also become a competitor in intelligence production. Intelligence consumers might be tempted to increasingly value the receipt of raw intelligence,⁷¹ which is not attached to analysis or assessments, and, consequently, function as their own analysts, as they 'collect and evaluate information themselves and are reluctant to accept wisdom from authority'.⁷² In this context, policymakers would try to create their own knowledge by filtering and merging information from multiple sources and providing meaning and context to them. Davis⁷³ believes that the amount of raw data, scholarly research, and open source media reports available to policymakers has led them to conduct their own research and analysis, which are often undertaken in a biased way. Their aim is to produce knowledge which sometimes supports their own preconceived position on a particular subject, especially when the IC fails to deliver products which support their position or fails to deliver innovative and convincing products. Thus, in order to avoid being marginalized, and therefore losing influence, power, and resources, intelligence professionals have been exposed to a growing pressure to provide decision-makers and their policy staff with tailored reports that are consistent with their 'analysis' and preconceived position on a specific issue,⁷⁴ which exponentially increases the risks of intelligence politicization. Coyne, Neal and Bell add that:

[t]he complexity of the international environment, the increased availability of information and data management tools, and historical intelligence theory have given rise to the concept of the client as an analyst. In the absence of a clear differentiation between policy and intelligence, analytical capabilities and roles, intelligence appears to be struggling to define its purpose in this post-modern information age.⁷⁵

It seems that this process has a strong tendency to engage intelligence customers in the intelligence business. This is far from being an ideal situation, since, among other aspects, policymakers do not have much time to devote to gathering and assessing information. Lock Johnson reports, for example, that 'some of the best assistant secretaries of defense and state have

⁷⁰Teitelbaun, *The Impact of the Information Revolution*, p.203.

⁷¹Walter Laqueur, *The Uses and Limits of Intelligence* (London: Transactions Publishers 2009).

⁷²Liaropoulos, A (R)evolution in Intelligence Affairs?, p.8.

⁷³Jack Davis, 'Tensions in Analyst-Policymaker Relations: Opinions, Facts and Evidence', Occasional Papers: Sherman Kent Centre for Intelligence Analysis, Vol. 2/2, 2003, pp.1-8.

⁷⁴Jack Davis, 'Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in Relationships', in Loch Johnson (ed.) *Strategic Intelligence: The Intelligence Cycle* (NY: Praeger 2007) pp.143-65.

⁷⁵Coyne, Neal and Bell, 'Reframing Intelligence', p.58.

conceded that they spent, at best, five minutes a day scanning intelligence reports; [...] Officials even higher in the policy hierarchy have even less time read intelligence reports'.⁷⁶ Considering that policymakers have a huge need to be informed, and scarce time to access information, they must carefully select their sources, paying attention only to those deemed valuable and reliable enough to be worth their time. Besides the time issue, it must be noted that as the mass of raw intelligence grows, it spawns worrisome problems for intelligence warning, analytical failures, manipulation of data and assessments by decision-makers, and politicization of intelligence. One should wonder, then, whether policymakers who consume raw intelligence master the analytical and methodological techniques needed to check and assess the veracity of reports, detect the possibility of purposeful deception, and systematically 'collate all source intelligence to thoroughly assess the validity and reliability'⁷⁷ of the information received.

Second, these possibly unmet customer needs open the door to a wide range of opportunities for 'information middleman services', who usually have the ability to: (1) undertake informed and efficient searches and direct customers/users to the specific information they need; (2) evaluate the validity for this piece of information, sometimes by consulting multiple corroborative sources; (3) fuse information from several sources and create a value added information product focused on the user's specific needs; and (4) perform all these tasks while being able to keep up-to-date on the continually proliferating information repositories throughout the world.⁷⁸

Thus, the sources policymakers rely on to obtain information and the nature of the information that they want/need appear to be the key elements to assess how the IR influences the way policymakers access and use information. In an age where knowledge, as well as the ready access to it, has become 'the decision maker's currency',⁷⁹ a policymaker's time is just too valuable to be spent on anything less than the most informative and essential information. However, in order to make their decisions, policymakers are more likely to trust in information coming from which sources? Considering the amount and importance of insights and knowledge that can be extracted from the vast repositories of publicly available information, decision-makers should not only be able to fully understand the existing differences among sources, the relationships among them, who collects and processes information – and how – but also where information is obtained and from whom. By doing so, policymakers can better value the importance of carefully processed intelligence and how it contributes to his knowledge of a national security issue. Lowenthal argues that:

⁷⁶Loch K. Johnson, 'A Framework for Strengthening US Intelligence', *Yale Journal of International Affairs* 1 (2006) pp.116–32.

⁷⁷Coyne, Neal and Bell, 'Reframing Intelligence', p.59.

⁷⁸Teitelbaun, *The Impact of the Information Revolution*, p.91.

⁷⁹Coyne, Neal and Bell, 'Reframing Intelligence', p.54.

[E]xternal intrusions, particularly that of the electronic news media, can have an effect on the relationship. [...] [I]t competes with the intelligence community as an alternative source of information. The media do occasionally scoop the intelligence community. This is not because they know things that the intelligence community does not. Instead the electronic media [...] put a premium on speed and have the capacity and willingness to provide updates and corrections as necessary. The intelligence community does not have the same luxury and tends to take more time in preparing its initial report. Being scooped by the media can lead policy makers to believe, mistakenly, that the media offer much the same coverage as the intelligence community – and at greater speed and less cost.⁸⁰

And what would the attributes of a good piece of information be? Although ‘information sharing’ used to be seen primarily as a government-to-government operation, policymakers are now widely receptive to government-private sector interaction. It means that policymakers might be more likely to dedicate their time and attention to sources of information which are able to apparently reduce the degree of uncertainty about a specific subject or event, and which do that in a saving-time manner for them, regardless of whether the potential source operates within government structures or outside it. Teitelbaun⁸¹ offers an extensive list of desirable attributes of information which would be most prized by policymakers and used as major criteria for choosing information sources:

1. **Timeliness:** It refers to the time elapsed since an event took place until the moment the source was able to provide the policymaker with the information;
2. **Perception of Accuracy/Reliability:** It refers to the reputation established by an information source for systematically providing information proven to be accurate and reliable. As to the information itself, accuracy can be seen as a measure of closeness between the type of information available to the type of information requested,⁸² reason why this trait is also known as *adequacy*. *Adequacy/accuracy* should be measured by ‘how well the product addresses and answers the specific concerns of an identified and targeted audience’,⁸³ which is essential, especially when one considers that, ideally, requirements should reflect policy makers’ prioritized intelligence needs;
3. **Ready Availability:** It means the degree of accessibility of an information source to a policymaker, or the extent to which the source makes the information available to the policymaker;

⁸⁰Lowenthal, *Intelligence from Secrets to Policy*, p.189.

⁸¹Teitelbaun, *The Impact of the Information Revolution*.

⁸²Newcomb and Hammell II, ‘Examining the Effects of the Value’.

⁸³Petersen, ‘What I Learned in 40 Years’, p.16.

4. **Ease of User Interface:** It refers to the level of difficulty presented to policymakers when using the source's interface to search and access information. The easier, the better;
5. **Speed of Operation:** It is intimately linked to timeliness, and measures how quickly the source is able to provide information once it is accessed;
6. **Flexibility of Use:** It refers to the ability of the source to allow the policymaker to store, duplicate, or in other ways use and keep the information;
7. **Capability:** It refers to a *qualitative* measure of the tools or utilities offered by the source to policymakers, to allow them to better use the information;
8. **Features and Function:** It refers to a *quantitative* measure of how many tools or utilities are offered by the source to policymakers, to allow them to better use the information;
9. **Comprehensiveness:** It refers to the breadth and depth of coverage provided by a source. Some scholars call this characteristic 'precision', understood as the level of detail provided by the information;⁸⁴
10. **Customer Support from Supplier:** It refers to the extent to which an information source will help a policymaker understand information or solve difficulties in using it.

Although all of these attributes are highly desirable, it appears that the major criteria for choosing information sources revolves around technical excellence of the content, understood as the combination of comprehensiveness, timeliness, accuracy/adequacy, and reliability. Secondary criteria include speed of operation, customer support, and ease of user interface. Also, the more tailored the information product, the more the consumer tends to value the service, which will save him time and attention.

At any rate, the success or failure of intelligence depends on the relationship between the IC and policymakers. Ideally, a clearly defined and harmonious relationship between these actors would be a prerequisite for achieving and maintaining desirable levels of efficiency in the intelligence activity. In the real world, however, the relationship between these actors tends to be fraught with tension, friction, miscommunication, and distrust – whose causes have a complex nature – especially when what is perceived as an 'intelligence failure' captures the attention of the media and the public. When an intelligence service allegedly fails to accomplish its expected missions and to offer an early warning to policymakers, who are caught by surprise by a strategic event which might result in an unforeseen security crisis, particularly dramatic consequences might take place and gain wide resonance.⁸⁵ This line of thought suggests that the causes of the failure to provide intelligence about threats or in providing only belated intelligence may be attributable in part to the lack of effective interaction between intelligence and policymakers.

⁸⁴Newcomb and Hammell II, 'Examining the Effects of the Value'.

⁸⁵John-Michael Arnold, 'Non-State-Led Strategic Surprise and US Foreign Policy: A New Variant of an Old Problem', *Yale Journal of International Affairs* 8/1 (2013) pp.1–13.

One of the main sources of friction is the non-formulation of priorities and requirements to an intelligence service. Intelligence is carried out on behalf of its customers – the decision-makers. Oftentimes, during the planning-and-direction phase of the intelligence cycle, decision-makers fail to clarify what kind of intelligence they need, for which purposes, and what questions they should pose,⁸⁶ leaving ‘intelligence officers [...] ignorant of the data desired by policy officials’.⁸⁷ What happens when requirements are not presented to the IC and policy makers do not define the priorities and queries? In this case, the IC will conduct the threat assessment process and establish intelligence priorities and policy requirements according to its own perception of both the domestic and international scenarios.

When this situation takes place, the intelligence service will likely be accused of participating in policy by taking an undesirable active role in the sphere of politics. Furthermore, when trying to determine what should be its priorities, in the absence of superior guidance and by relying only on its own experience and expertise, an intelligence service risks making mistakes and organizing purposeless intelligence activity, which leads to what some scholars believe to be the problem of irrelevance of intelligence,⁸⁸ not to mention the waste of time and human and economic resources. In that regard, Loch Johnson notes that ‘[a]ll too often policymakers scrawl “irrelevant” or “OBE” (overtaken by events) in ink across intelligence reports’.⁸⁹ In consequence, state institutions and individuals that fail to establish the priorities, present tasks, or influence intelligence activity in any other way should share the responsibility for intelligence failures. It must be noted, however, that this situation seems to fit what Treverton calls *real intelligence cycle*, which is basically driven by ‘intelligence pushing’ rather than by ‘policy pulling’,⁹⁰ and which excludes the decision-maker from the process. In his model, as the policymaker does not have time or patience to formulate his requirements, the IC detects its demands and goes about its tasks.

Problems between the IC and decision-makers may also arise due to the absence of feedback. It would be a mistake to believe that the process of intelligence is over when an intelligence service of a democratic state delivers its product to their appropriate customers. The role of politicians and decision-makers regarding intelligence services is not limited to receiving intelligence information. In the final analysis, they decide what they want to receive, what will be relevant or not, how, why, and when. In Lowenthal’s words, ‘they shape it’.⁹¹ In the intelligence process, not only is the timely

⁸⁶Tom Quiggin, *Seeing the Invisible: National Security in an Uncertain Age* (Singapore: World Scientific Publishing 2007).

⁸⁷Johnson, ‘A Framework for Strengthening US Intelligence’, p.117.

⁸⁸Gintaras Bagdonas, ‘Relations between Intelligence Services and Policy Makers: An Analysis of Challenges and Their Causes’, *Lithuanian Annual Strategic Review*, 2008, pp.9–28.

⁸⁹Johnson, ‘A Framework for Strengthening US Intelligence’, p.118.

⁹⁰Treverton, *Reshaping National Intelligence*.

⁹¹Lowenthal, *Intelligence from Secrets to Policy*, p.174.

receipt of priorities and requirements of utmost importance, but also feedback. If feedback is not systematically provided, an intelligence service will be left in obscurity and will not be able to properly evaluate its potential mistakes. It may not even know whether there was any mistake. And, considering that intelligence is more about putting facts in perspective than about having command of the facts,⁹² dealing with uncertainty, ambiguity, and incomplete or unavailable information, the IC can make mistakes, which is not absolutely unforgivable. Ford, for example, argues that the main problem with intelligence analyses of Iraqi weapons of mass destruction before the US invasion in 2003 was not that they were wrong, neither was the fact that the policy community arguably compelled flawed analysis in order to justify predetermined policy goals. The problem was that policymakers accepted the conclusions of the IC without a second thought and without providing feedback.⁹³

An ideal situation would be one in which, time allowing, after presenting its first product to clients, an intelligence service receives additional questions and continues the intelligence process by going deeper into the problem and proceeding into a second 'circle' or 'round' of the intelligence process. The final product would be one more tailored to a customer's needs. At the same time, due to the feedback provided by the intelligence customers, not only the product of intelligence and its format are likely to be improved, but also a better understanding on the decision-makers' needs and objectives can be reached. This could be the result of a constructive relationship characterized by 'a slightly skeptical, probing sort of substantive engagement [which] requires efforts and understanding from both sides'.⁹⁴

A clear understanding on the part of policymakers about what the IC can and cannot do is a central element in these relations.⁹⁵ As a former intelligence officer once noted, 'no small part of the disillusionment policymakers have had with intelligence is that they [...] have inflated and unrealistic expectations about what the Intelligence Community can do'.⁹⁶ Part of these heightened expectations comes from the large availability of data and sophisticated analyses made possible by the IR, in a context in which policymakers expect more from the IC than what is produced by private information brokers, think tanks, journalists, and the social media. Likewise, policymakers must understand the relative roles of open source and traditional intelligence in meeting their needs. Actually, both sides must necessarily understand each other's duties, responsibilities, limitations, and abilities. In the absence of this type of understanding, conflicts are likely to emerge. As Laqueur says: 'Intelligence not only has to train new recruits but

⁹²Petersen, 'What I Learned in 40 Years'.

⁹³Christopher A. Ford, *Relations between Intelligence Analysts and Policymakers: Lessons of Iraq* (Washington, DC: Hudson Institute 2009).

⁹⁴*Ibid.*, p.3.

⁹⁵Bagdonas, 'Relations between Intelligence Services and Policy Makers', p.8.

⁹⁶John Gentry, A Framework for Reform of the US Intelligence Community, 1995 <www.fas.org/irp/gentry/index/html>

also to educate its customers. This is a formidable task because the latter, at a more advanced age, are very busy people, sure of their own judgment [...]. They have to be convinced of what intelligence can, and what it cannot, achieve'.⁹⁷

The interaction between the IC and decision-makers must be reciprocal. Intelligence officers must necessarily understand how the 'world of politics' works. Davis suggests that they have to become experts of the state's politics so they can see the world through the eyes of policymakers. On the other hand, decision-makers are supposed to facilitate the work of intelligence officers by allowing them to be informed about political decision, which means that intelligence officers should be incorporated into the decision-making process, discussing with policymakers their information needs, and learning 'from the inside how they can help with timely factual information and objective analysis'.⁹⁸ Some fear that if intelligence officers were responsible for not only providing intelligence, but also for suggesting developments on decisions of policy that arises from the provided intelligence, the IC might submerge in the sphere of politics. Intelligence would become politicized and its products biased.⁹⁹ However, if intelligence officers have no real access to policymakers, then their product, and the whole intelligence activity, tends to become less relevant to the immediate agendas of policymakers. By contrast, policymakers who do not devote time on a regular basis to read intelligence reports, and question them if necessary, are clearly not doing their jobs.

A persistent problem in the IC has been the inability of senior leaders to view their enterprise as a business with definable products and clients with particular demands. Satisfying these demands should always be the primary objective of the IC. This is not possible, however, without guidance and feedback. Allen W. Dulles, CIA Director between 1953 and 1961, acknowledged that even the best planner and head of intelligence cannot foresee everything.¹⁰⁰ For this reason, he believed that precise guidance and systematic feedback are possibly the most important, but also the most challenging, parts of the intelligence process.

Conclusions

The advent of the IR has had a deep impact upon the intelligence cycle, upon the way the IC works and how it interacts with decision-makers. To some, it also has displaced the pre-eminence of intelligence in decision-making, as it is arguably less clear to the policymaker what intelligence is and what unique service or product it provides. The IR also affected the way policymakers access reliable information and what sources they are most likely to rely on. As Betts notes, 'in recent times, the prominence of "real-time" news reporting

⁹⁷Laqueur, *The Uses and Limits of Intelligence*.

⁹⁸Johnson, 'A Framework for Strengthening US Intelligence', p.130.

⁹⁹Davis, 'Intelligence Analysts and Policy Makers'.

¹⁰⁰Allen W. Dulles, *The Craft of Intelligence* (Guilford, CT: The Lyons Press 2006).

from CNN further draws policymakers away from carefully processed intelligence'.¹⁰¹

Until recently, decision-makers were highly dependent on the products provided by the IC. However, the IR has allowed individuals to obtain an ever expanding quantity and variety of information from the most distinct sources, some of which can provide sophisticated analyses. The combined power of globalization and the internet has spread knowledge and enabled public access to information that governments and the IC once viewed as secret intelligence. The evolution of classified intelligence systems and databases has moved immediate access to holdings of raw information and intelligence product, from intelligence units/cells, directly to the decision-maker's laptop¹⁰². Furthermore, front-end interfaces and back-end information searching capabilities have become more simplified and intuitive, resulting in an arguably more informed decision-maker.

The complexity of the international scenario, coupled to the wide availability of information and the development of new data management tools, has given rise to the concept of the decision-maker/client as an analyst, in a context where, to the eyes of many critics, the IC appears to be struggling to define its purpose in this post-modern information age. As it was exposed, intelligence customers tend to increasingly value the receipt of timely raw secret intelligence, which has undergone only limited analytical review and evaluation, often 'at the cost of more detailed analytical products'.¹⁰³ In fact, all around the world private businesses are increasingly offering their own 'competitive intelligence' services to advise their clients, which require the development of sophisticated methodologies to gather and analyze information tailored to specific users. However, all these developments are nowhere close to eliminating the need for traditional intelligence provided by official structures. The adoption and use of intelligence as a strategic planning tool, which is very common in the government sphere, is a capability that not many private companies have been able to fully master for a variety of reasons, including their legal incapacity to conduct secret intelligence operations, which are limited by law to government authorities. Furthermore, do decision-makers who use such raw intelligence understand the limitations faced by private brokers regarding technical collection capabilities? Are they able to check and assess the veracity of reports, detect the possibility of deliberate deception, and systematically integrate data from various sources to assess the validity and reliability of the information received? Even though some argue that the value of intelligence sources and methods may be declining in a more open world to where they must compete for policymakers' attention, the answers to these questions help to explain why the value of intelligence has not yet been crowded out by non-

¹⁰¹Richard Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York, NY: Columbia University Press 2007).

¹⁰²Lowenthal, *Intelligence*.

¹⁰³Coyne, Neal and Bell, 'Reframing Intelligence', p.58.

intelligence sources. The role of the intelligence professional and the value the IC can provide go much beyond the mere collection of secret intelligence.

The IC and the intelligence professional will not become irrelevant and, as important as it is, *open sourcing* will not replace traditional intelligence. Indeed, in order to catch up with the frenetic pace of the changes in global affairs and the world news cycle, policymakers will probably increase their demand of knowledge from the IC. As the volume of information and their sources multiply, policymakers' needs for processing and analyses will also increase, one reason why they will continue expecting the IC to play its central role in extracting needed information from other governments and actors, while protecting their own secrets from being stolen. Yet, since policymakers can now have access to open sources as readily as the IC, they will expect the open source information to be quickly validated by the IC and rapidly meld with the information obtained from traditional sources of collection, so that they can acquire the knowledge desired. Then, to meet the heightened expectations of policymakers, and in the face of the power of technology to gather raw data very rapidly, the IC must constantly reinvent itself, assimilating new and more dynamic information technologies and collection capabilities, managing information overload, developing and perfecting *social intelligence* skills, using alternative methods of analysis, increasing and improving long-term analyses, reinvigorating the use of HUMINT, and adapting processes and means of conveying its product to policymakers.

The IR is an ongoing process, which is far from over and which has redefined the way intelligence is used and conceived. Likewise, the intelligence activity is in a transition phase, in which the intelligence officer has been provided with – and challenged by – new technological tools, while new ideas, perspectives, methods, and concepts have been applied in the intelligence cycle. Although the craft of intelligence has fundamentally remained the same, the IC needs to be constantly adapting to the technological, organizational, and cultural challenges that it has brought about. In this context, readdressing the relationship between analysts and consumers, making the best of open source information, and speeding up the development of collection protocols regarding online social networks are some of the challenges that intelligence currently faces and needs to overcome, if it wants to safeguard its preeminent role in providing intelligence to decision-makers and remain the country's first line of defence against threats to national security and interests.

Disclosure statement

No potential conflict of interest was reported by the author.

Notes on Contributor

Marcos Degaut is a Brazilian Political Advisor at the House of Representatives and former Intelligence Officer. He served as Assessor to

International Affairs at Brazil's Institutional Security Cabinet, as Deputy Head of International Affairs at the Superior Court of Justice, and as Secretary General of the National School of Magistrates (ENFAM). He is currently a PhD student in Security Studies at the University of Central Florida.