

Current Intelligence and Assessments: Information Flows and the Tension between Quality and Speed

Mikael Weissmann & Niklas Nilsson

To cite this article: Mikael Weissmann & Niklas Nilsson (01 Feb 2024): Current Intelligence and Assessments: Information Flows and the Tension between Quality and Speed, International Journal of Intelligence and CounterIntelligence, DOI: [10.1080/08850607.2023.2296886](https://doi.org/10.1080/08850607.2023.2296886)

To link to this article: <https://doi.org/10.1080/08850607.2023.2296886>



© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC



Published online: 01 Feb 2024.



Submit your article to this journal [↗](#)



Article views: 173



View related articles [↗](#)



View Crossmark data [↗](#)

MIKAEL WEISSMANN AND NIKLAS NILSSON

Current Intelligence and Assessments: Information Flows and the Tension between Quality and Speed

Abstract: This article takes a particular interest in the dynamics between information flows, continuous ongoing assessments, intelligence dissemination, and forward-looking operational advice. The point of departure is the tension between balancing quality (in the sense of in-depth processing of large amounts of information) and speed (meeting requirements of timeliness) in current intelligence assessments. The article takes an explorative approach to practices in current intelligence, utilizing qualitative interview data combined with open source material.

The radically improved access to information through a wide variety of means over the last decades has given rise to both advantages and challenges for the practice of intelligence. Advantages include the fact that much

Mikael Weissmann is an Associate Professor in War Studies and the Deputy Head of the Land Operations Division at the Swedish Defence University's Department of War Studies. He is the co-convenor of the Hybrid Threats Research Group and the Land Warfare Research Group, as well as the Principal Investigator of the project "Building Resilience and Psychological Defence: Countering Hybrid Threats and Foreign Influence and Interference." He is co-editor of the books Russian Warfare and Influence: States in the Intersection Between East and West (Bloomsbury Academic, 2024), Advanced Land Warfare: Tactics and Operations (Oxford University Press, 2023), and Hybrid Warfare: Security and Asymmetric Conflict in International Relations (I.B. Tauris, 2021). The author can be contacted at mikael.weissmann@fhs.se.

© 2024 The Author(s). Published with license by Taylor & Francis Group, LLC.

This is an Open Access article distributed under the terms of the Creative Commons Attribution-NonCommercial License (<http://creativecommons.org/licenses/by-nc/4.0/>), which permits unrestricted non-commercial use, distribution, and reproduction in any medium, provided the original work is properly cited. The terms on which this article has been published allow the posting of the Accepted Manuscript in a repository by the author(s) or with their consent.

information that was previously costly, resource-intensive, and often dangerous to obtain is now more or less freely available. However, the flipside of this development is a range of challenges due to the changing signal-to-noise ratio, requiring vast collection and processing in order to identify relevant pieces of information. While this can be considered a challenge common to the Intelligence Community (IC) at large, it arguably becomes especially pronounced in the time-sensitive practice of current intelligence analysis. Problems related to current intelligence are a less explored topic in the field of Intelligence Studies compared to, for example, strategic intelligence. However, it is arguably in the practice of current intelligence that the dilemma and tradeoff between producing intelligence of the highest possible quality, and doing so within short timeframes, becomes particularly acute.

This article focuses on practical challenges for the production and communication of current intelligence in the context of a rapidly expanding information environment. It takes a particular interest in the dynamics between information flows, continuous ongoing assessments, intelligence dissemination, and forward-looking operational advice. The point of departure is the tension between balancing quality (in the sense of in-depth processing of large amounts of information) and speed (meeting requirements of timeliness) in current intelligence assessments. The article takes an explorative approach to practices in current intelligence, utilizing qualitative interview data combined with open source material. The firsthand empirical data presented in the article were collected through semistructured and discussion-style interviews with experts, former insiders, researchers, and other informants, with experience from intelligence agencies in Western Europe and the United States. The data that are utilized to identify common denominators with general relevance

Niklas Nilsson is Associate Professor in War Studies at the Swedish Defence University, where he holds positions at the Land Operations Division, Department of War Studies, and the Centre for Societal Security. He is a co-convenor of the Hybrid Threats Research Group and the Land Warfare Research Group. He is the lead editor of the forthcoming book Russian Warfare and Influence: States in the Intersection between the East and West and co-editor of the recently published books Advanced Land Warfare: Tactics and Operations (Oxford University Press, 2023) and Hybrid Warfare: Security and Asymmetric Conflict in International Relations (I.B. Tauris, 2021). The author can be contacted at niklas.nilsson@fse.se.

The views and opinions presented in this article are those of the authors alone, and do not necessarily represent those of the Swedish Armed Forces or the Swedish Defence University.

thus represent perspectives from a range of different backgrounds and experiences from different countries and agencies, The interview respondents have been anonymized.

The article is structured as follows. First, we discuss challenges relating to the conduct of intelligence in the increasingly abundant information environment, and the particular constraints these place on the practice of current intelligence in light of time constraints and requirements for timely assessment. We then present three main themes emerging from the interviews, which are identified as particularly salient in relation to current intelligence. The themes are *information availability and producer–consumer relations*, *speed versus quality*, and *artificial intelligence (AI)–powered information management*.

INTELLIGENCE AND INFORMATION ABUNDANCE

Information flows naturally play a critical role in intelligence analysis. Good access to timely and relevant information is not least important when it comes to meeting policymakers' needs for prompt and accurate intelligence. As Amy Zegart has pointed out, "Satisfying policymakers' need for speed while carefully collecting, vetting, and assessing intelligence has always been a delicate balance, but that balance is getting harder to strike."¹ For example, during the Iraq War, it became clear that the traditional methods of intelligence analysis that had been developed during the Cold War did not meet the demands of wartime intelligence. In order to cope with the massive increase in intelligence data, new analytical tools had to be adopted that could identify and link key developments and the people hidden within them.²

One parameter that has become increasingly evident in the resolution of this task is the exponential increase in information flows over the past decades. Whereas the availability of potentially important information has increased dramatically, the prioritization, processing, and analysis of virtually unlimited amounts of information have become increasingly resource-intensive.

This exponential increase in data volume and velocity is derived from both open source and covert platforms that have disrupted and transformed intelligence operations. This creates new demands on technology, which can be helpful for augmenting human cognition through a combination of high-performance computing and AI, which together enhance the IC's capacity to identify, synthesize, and take action on the essential information elements pertinent within the data.³

Technology has been a key accelerator for information flows, as computational propaganda has been increasingly used by actors.⁴ For example, the use of junk news backed by automation and the use of bots

creating a powerful set of tools for actors using digital disinformation.⁵ In short, the importance of understanding the dynamics of information flows affected by automated systems and the impact they have on intelligence analysis is not only larger than ever but increasing.

Information flows are critical to intelligence analysis and form the basis for obtaining fair and accurate intelligence at the right time. The challenges posed by the increasing volume and velocity of data, digital disinformation, and the need for augmented cognition require intelligence professionals to adapt their tools and methods. By embracing new analytical techniques, understanding the effects of computer propaganda, and leveraging AI, the IC can navigate the complex flow of information and deliver actionable insights to decisionmakers.

Operational assessment work requires tools to manage the dynamics between information flows, continuous assessment, information spillover, and forward-looking operational advice in an environment of virtually unlimited information. The intelligence and security services must ensure that they have or acquire the appropriate means for handling the dynamics between information availability, assessments, and dissemination in an environment with formerly unimaginable data volumes. Furthermore, the exponential increase and volatility of information flows demand a continuous development of existing tools and methods for these to remain relevant in the future operating environment.

The variety of potential sources is in part demonstrated by the growing number of “ints” in the intelligence world. These include human intelligence (HUMINT), signals intelligence, communications intelligence, imagery intelligence, geospatial intelligence, measurement and signatures intelligence, and open source intelligence (OSINT).⁶ Additionally, social media intelligence (SOCMINT) has emerged as the latest member of the intelligence family. To cite Omand, Bartlett, and Miller, “In an age of ubiquitous social media it is the responsibility of the security community to admit SOCMINT into the national intelligence framework.”⁷

The exponential increase in the flow of information has thus created significant challenges for the IC. The challenges of collection, processing, and dissemination of information and intelligence and their place and role in the planning process as well as continuous assessment and adaptation or flexibility in operations must be addressed to ensure the effective functioning of intelligence services.

CURRENT INTELLIGENCE, TIME CONSTRAINTS, AND TIMELY ASSESSMENT

Aside from required adaptation in terms of intelligence collection and analysis capacity, these requirements run up against particular challenges in

relation to available time. The (sometimes contradictory) relationship between imperatives of producing high-quality intelligence assessments and time constraints is present in most intelligence work.⁸

We define intelligence as a corporate capability to forecast change in time to do something about it. The capability involves foresight and insight, and is intended to identify impending change, which may be positive, representing opportunity, or negative, representing threat.⁹ The article's understanding of intelligence analysis, in turn, follows Gentry and Gordon's outline of four core functions of intelligence analysis¹⁰: (1) strategic warning, (2) basic research (or strategic) intelligence, (3) estimative intelligence, and (4) current intelligence. While the issue of time scarcity is present across these functions, it becomes particularly salient in the category of current intelligence, which is the primary focus of this article. Hence, we are interested in the process of assessing and communicating intelligence based on the information available at specific points in time, in the face of an imminent threat or decision point.

Current intelligence is characterized by its preoccupation with "issues that require immediate attention" and is often "disseminated quickly, with a minimal level of evaluation or interpretation."¹¹ The growth in available information, giving rise to what is sometimes described as a "fog of information problem," becomes a particularly salient problem to manage for current intelligence analysts, given the short timeframes available for sorting and processing information. Striking the balance between speed and quality therefore takes on special features, delimiting the room for analyzing and processing incoming information, and often inducing a need to prioritize speed over quality. In turn, this implies that uncertainty, which is also arguably a factor in all intelligence work, is more prevalent in current intelligence given the need for fast dissemination of intelligence over short time horizons. In this sense, the process of collecting, analyzing, disseminating, and taking decisions based on current intelligence can be likened to the defining features of a crisis, frequently described as a perceived threat that needs to be addressed, high levels of uncertainty, and time constraints.¹² Thus, similarly to judgment calls regarding current intelligence assessments, crises give rise to a decisionmaking environment with limited time to collect and process information and a strong sense of urgency, where quick decisions must be made based on the knowledge at hand.¹³

Current intelligence is frequently connected with tactical intelligence, often in a military perspective and as primarily in support of ongoing military operations. Yet, while this is certainly a core utility of current intelligence,¹⁴ we argue that the judgment calls regarding time versus quality, uncertainty, and the imperative to produce the best possible assessments at given points in time are transferrable across levels of

analysis and work equally well at the strategic level. Indeed, the delimitation between different fields of intelligence is becoming increasingly blurred, along with the increasing complexity of the security environment as well as the IC itself. As Odom has pointed out,

the Intelligence Community is far more diversified in its tasks than is generally realized. Where analysis is done and for whom makes a large difference in its effectiveness. Moreover, changing technology is altering how it is done, where, and by whom. The border between what is “strategic” or “national” intelligence and “tactical” intelligence is much diminished.¹⁵

The analysis focuses on the production and delivery of intelligence assessments, the point at which accumulated knowledge (processed and analyzed intelligence) must be packaged and communicated to intelligence consumers. Intelligence assessments can be understood as the establishment of the best possible knowledge of a situation at a particular point in time, which in turn orients the decisionmaker regarding possible and preferable lines of action. In other words, the intelligence assessment is what moves something from planning and preparation to a course of action. The presentation of this “output” may take different forms depending on the needs of the decisionmaker—it may be a publication in the form of a written text or handout, or simply a verbal presentation. Yet, as will be demonstrated below, the changing information environment raises particular challenges in the interaction between producers and consumers.

We now proceed to discussing three themes identified in the interview data as being of particular importance, and raising important challenges, in relation to the tradeoff between quality and speed in light of the changing information environment. While these themes have general relevance for different types of intelligence, they have particularly important consequences for current intelligence given the time compression involved. The themes concern, first, the abundance of information available to intelligence agencies as well as decisionmakers, and aspects of how this affects the relationship between them. Second, the issues of time, information, and the internal workings of and practices employed by intelligence agencies, particularly relating to tolerance for risk and uncertainty as well as methods for analysis. Third, implications of the AI revolution and its potential to both address the problem of information overload and create new issues and challenges. In this regard, the data provide some perspectives on the challenges emerging for intelligence agencies in employing these technologies and the extent to which this implies a substantial shift in allocation of resources and competencies.

INFORMATION AVAILABILITY AND INTELLIGENCE PRODUCER–CONSUMER RELATIONS

The relationship between the intelligence producer and consumer is a well-known topic in intelligence studies. Many of the factors applying to this relationship that relate to the impact and productive utilization of intelligence in pursuit of security and political objectives are generic and apply to all thinkable types of intelligence. Yet there are certain features of current intelligence in relation to the increasing accessibility of information and the often very short timeframes involved that have a particular impact on this relationship. This pertains particularly to the growth in information available to intelligence consumers independent of intelligence agencies, via social media and other sources.¹⁶

The ever-increasing availability of open source and social media data has contributed to an information environment that is often depicted as revolutionizing intelligence. Rough estimates indicate that 80% of all information that goes into intelligence analysis is based on open information, although the share can be both smaller and larger.¹⁷ Observations regarding the extensive open source coverage of Russia's full-scale invasion of Ukraine indicate the extent to which information, often of significant intelligence value, becomes accessible through open sources. The backdrop, however, is that the material produced by a very large number of sensors, including commercial satellites, civilians using mobile phones, and disclosed material produced by military personnel, is extremely extensive.

Judgments on the utility of open source information in intelligence have shifted in writings on the subject, from prophesizing the end of traditional intelligence, to rendering OSINT of little value in comparison to information collected via covert means, to questioning whether the term OSINT in itself is at all useful.¹⁸ Views differ between insiders and outsiders, where intelligence practitioners tend to take a balanced and cautious view on the subject. While no one questions the expansion of open source and social media information, there has sometimes been a skepticism regarding its actual usefulness, which has been exemplified in certain organizations having shown a strong aversion to using open sources.¹⁹

In the interviews conducted for this article, several interviewees pointed to a problem arising as the speed with which open source information spreads raises challenges regarding both the ability to add value in current intelligence assessments, and the imposition of unproductive time constraints and micromanagement due to information availability.

According to one respondent, referring to a previous assignment, "We had an OSINT cell, they did a great job, but mainly reported the news." The intelligence value of this was questionable, because the senior officers who were in receipt of the intelligence had the same information feed in their

systems.²⁰ Other respondents pointed to the fact that because so much information is openly available, it becomes easy and tempting for intelligence consumers to attempt to conduct their own analysis. Consumers therefore frequently think they know more than they actually do, based on analysis that is not professionally conducted.²¹ It can also create the impression that intelligence agencies are slow given the time required to subject information to fact-checking and counterfactual analysis. In turn, consumers can be incentivized to pose pointed questions regarding delimited areas, which can steer resources into areas that may not otherwise be logical priorities in the overall collection effort. Moreover, this logic risks providing for a reactive approach to intelligence collection and analysis, where time limitations become unnecessarily constrained and where quality is deprioritized.²²

These features of intelligence work raise questions about the future role of intelligence agencies in an age defined by an exponential growth in the availability of “big data” and open sources. Whereas none of the respondents questioned the future utility of intelligence agencies per se, several highlighted that their role was changing and that the changing information space posits a challenge of explaining the “added value” of intelligence. The value added by combining different sources will always be relatively slower. Several interviewees argued that these tendencies speak to a general requirement in the IC to educate intelligence consumers by demonstrating and arguing for the value of its service and that it “adds something to the table.”²³

Rather than reporting already accessible information, the value of intelligence is in showing what happens, what it means, and what it means to the consumer.²⁴ This challenge also clearly ties into expectation management, as an additional pedagogical task lies in clarifying what intelligence consumers can expect and what they get—in other words, conveying the uncertainties involved in intelligence assessments.²⁵ This relates to helping consumers understand existing capabilities, but also how to ask questions.²⁶ Part of the problem is to get the consumer to understand that intelligence analysis does not only consist of relaying news reports or social media feeds, even though much information can be looked up in databases or online. While they might think they can do their own analysis, intelligence agencies have professional expertise that consumers tend not to have. At the same time, analysts must also have the confidence to tell consumers that something cannot be done, and to be frank about what they can and cannot do.²⁷ Moreover, while current intelligence analysis requires action as soon as something happens, if only to show the value of intelligence, there needs to be an understanding from the consumer that they cannot always expect a finished analysis if what has happened falls outside the area you have been delegated (even though ideally intelligence should have anticipated that need).

The flipside of the educational problem described above is the need for intelligence agencies to understand their consumers—their actual needs and how they operate, regardless of who the consumer is.²⁸ One respondent described relations with the consumer as “... a huge part of it. You have to understand their world view, how they plan to interact with the environment.”²⁹ Thus, the “battle rhythm” and decision cycle of the consumer is a necessary consideration in intelligence analysis, because policy advice at the wrong time is both less useful and risks being a waste of the limited time of the intelligence analyst. The respondents brought up several examples where consumer decision cycles were not in sync with their requests for intelligence reports.³⁰

Ideally, therefore, an efficient and optimized intelligence process should build on a well-established mutual understanding between intelligence producers and consumers of their respective preconditions and requirements. Several respondents pointed to tendencies of micromanagement by tasking intelligence agencies with responding to far too narrow questions as a signifier of an unproductive relationship in this regard. On the contrary, the delegation of collection and analysis based on a broader conception of the problem to be addressed denotes mutual understanding and trust. The key point in this line of reasoning is that the intelligence consumer rarely knows precisely what they want and need and therefore is not in a position to define narrow target areas for collection. As put by a former senior UK intelligence official, “Do not ask us a question, tell us what the problem is.”³¹ Moreover, as is the case with intelligence analysis in general, current intelligence analysis must be placed in its appropriate context in order to be meaningful and optimized.

A productive relationship between intelligence agencies and consumers should thus ideally be defined by interaction and communication.³² Yet the proposition that such a relationship needs to be defined by mutual trust and understanding of consumer needs is not always achievable in practice. One U.S. respondent argued that the idealized situation in which the analyst will interact with and receive feedback from the consumer is true only at very senior levels, whereas the vast majority of analysts will have little knowledge of what happens with their reporting once it is released and whether consumers consider it to be useful.³³

While this may be a generic feature of intelligence work, it is arguably especially pertinent in the vast U.S. IC. Indeed, the perspective differs in smaller states with far less resources devoted to intelligence, which is an important distinction because the bulk of intelligence research draws on the U.S. IC with its unique capabilities. The distance between analysts and consumers naturally increases in tandem with size, and in the United States this distance is often immense.³⁴ In smaller states, even junior analysts may

very well have been in contact with their minister of defense, prime minister, or supreme commander, or at least their immediate superiors have.

SPEED VERSUS QUALITY: TIME PRESSURE IN INTELLIGENCE ANALYSIS

Striking the balance between speed (the delivery of time-sensitive intelligence assessments when these are due) and quality (ensuring that the assessment represents the best possible knowledge at that particular point in time) is yet another generic feature of intelligence work that becomes particularly salient in the context of current intelligence.³⁵ Indeed, one respondent referred to current intelligence as being especially subjected to the “tyranny of the immediate,” a constant tension between the need to produce the best possible intelligence products and doing so in a timely manner.³⁶

This raises a particular set of demands on intelligence production under time pressure. First, it invites analytical shortcuts, because most structured analytical techniques (SATs) that analysts are trained to use do not lend themselves to coherent application within very short timeframes. SATs are methods developed in order to avoid analytical traps and biases. Yet their application requires time, which is often not available in situations where much depends on the analyst’s ability to evaluate information quickly. As put by one respondent, “[A]ny analytic office I have been in, they know these techniques and how to use them, but never had the time to use them.”³⁷ Instead, time pressure frequently leaves the analyst to make judgment calls regarding what new information means and how it fits into a larger context relying on intuition and gut feeling.

Experienced analysts may have a developed intuition based on long experience, deep knowledge, and techniques they have practiced in their career. However, the apparent necessity of relying on the individual analyst’s ability to evaluate information may necessitate a different approach to training and the teaching of SATs, particularly for analysts engaging in current or tactical intelligence. One respondent argued that a heavier emphasis should be put on proficiency in critical thinking, training analysts to determine “that this is what’s important, here’s how to recognize the biases in my own thinking, here’s how to ask myself, am I looking at enough of the information, at the right information, am I putting it into an appropriate context, does it all make sense.”³⁸ Time constraints also induce analysts to develop some favorite SATs, as it takes time to learn new ones and that time is rarely, if ever, available. In this regard, as argued by one respondent, the analyst needs to invest in a basic set of tools that are “good enough” (i.e., providing sufficient accuracy for the purpose or task at hand), in order to assess information quickly and to avoid biases, and needs to be aware of the shortcuts taken in the analysis.³⁹

Second, the requirement of timeliness implies that the best possible intelligence assessments at specific points in time will represent at best incomplete and at worst misleading depictions of reality, which may need to be revised or discarded in light of new information. In turn, this requires that analysts are both capable of managing uncertainty and of accepting risk. Ultimately, the risk involved for the individual analyst lies in producing an analysis that turns out to be wrong. Many analysts, according to one respondent, “loathe to say something when they are not certain [even though being] ninety per cent right and getting the information to the decisionmakers in time is better” than being correct but too late.⁴⁰

Consequently, to be able to make pinpointed and timely judgments of a situation it is important to accept the risk of being wrong, because excessive risk aversion risks leading to paralysis and inefficiency. Here the organizational culture in which analysts operate plays an important role in shaping the preconditions for producing accurate and useful intelligence.⁴¹ This culture needs to be permissive of mistakes—ideally, analysts should be allowed to operate under circumstances where occasional mistakes are considered an unavoidable occurrence in their work, and where both successes and failures are utilized for learning and improvement of the analytic process.⁴²

AI-POWERED INFORMATION MANAGEMENT

An area that is acquiring increasing attention in intelligence studies and that is frequently highlighted as a potential solution to the problems associated with extensive information availability and time constraints is the very rapid development of new technologies in AI and machine learning (ML). Western defense forces and their intelligence and security services are investing heavily in this field. For example, the U.S. Department of Defense increased its open investments in AI from just over \$600 million in 2016 to \$927 million in 2020, with a total of over 600 reported active AI projects.⁴³ While it is far from clear that AI-supported information management and analysis is the solution to all problems, AI is bound to play both a central and needed role in the management of the growing volumes of information and data.

One question here is whether ML/AI is in fact better at gathering information. Several of the interviewees do not believe it can beat human analysts in intelligence gathering, in part because this is a process that requires intuition and because the human environment cannot be fully grasped by machines. These risk missing out on both dimensions and factors that only a human can grasp when it comes to questions pertaining to “What are humans going to do?”⁴⁴ Furthermore, there are also questions of oversight and accountability, as well as ethics, that are problematic in relation to AI. This said, there is an acceptance that when it comes to trend

analysis and ability to look for the needle in the haystack, the introduction of AI-supported analysis holds significant promise.

Yet, while AI can be of great assistance in managing large data volumes, one should not place inordinate faith in big data. Big data in itself is of limited value unless appropriate algorithms are designed catering to the needs of the analysts. There is also a need for structured data to make accurate analysis. As one former senior U.S. official argued, there is a tendency to think that if we just get big data, we will have all this information and we can find all those nuggets of information that we will otherwise miss. Yet, while there is certainly truth to this, too many people do not think about what you need to do to succeed with this.⁴⁵

It is clear from the interviews that the view on the role of data analysis and AI is varied among experts and insiders. Some do perceive data analysis and AI as being a threat, while others instead think it could open up more space for people to think about bigger issues as more rudimentary, and tedious tasks are done by the machines. It has also been suggested that the support of technology may create more time for analysts to tackle soft issues that are not clearly quantifiable, but still often are crucial factors. One such example would be the assessment of operational capabilities of your opponent's military forces, where only counting measurable assets will risk creating a flawed conclusion.

Another problem with data analysis and AI relates to understanding the algorithms. It is of little use, even dangerous, that the machines may be brilliant at handling big data if the analysts do not understand the algorithms behind the analysis. The analyst needs not only to understand the limits and constraints of the results and conclusions drawn but also to be able to channel pedagogically their understanding to the consumers. As one of the interviewees pointed out, the big question is how to build trust into the algorithms, making the consumers confident in the system, noting that there is no simple solution to build the trust needed to give consumers confidence in the systems.⁴⁶

CONCLUSION

This article has explored a set of important challenges emerging as the quality and reliability of intelligence assessments need to be weighed against speed requirements in the context of an ever-growing abundance of information. While striking this balance is to a larger or lesser extent a challenge common to all strands of intelligence, regardless of their level of analysis or timeframe, it arguably becomes particularly important in highly time-sensitive current intelligence work. Our findings demonstrate important aspects of how the rapidly expanding information environment presents both advantages and challenges for the production and communication of current intelligence.

The information revolution, coupled with technological breakthroughs, has resulted in an exponential increase in data volumes and data velocity, from open as well as covert sources, which have in turn revolutionized the preconditions for intelligence production. Yet this fact also poses important challenges and questions regarding the role and function of intelligence agencies and professionals in the national security architecture. This emerging reality is affecting change and evolution in the organization, methodologies and staffing of intelligence agencies, although to varying degrees, while it also has consequences for the relationship between intelligence producers and consumers. The same realities that greatly simplify access to information for the intelligence producer also make large parts of the information readily available to consumers. Several respondent accounts highlight how this frequently gives rise to duplication of efforts and micromanagement. Consequently, the expanded information availability imparts an important pedagogical challenge to intelligence agencies worldwide—to demonstrate to intelligence consumers how the expertise and analytical capabilities of intelligence professionals contribute insights and verified knowledge beyond mere access to information. In other words, intelligence agencies must make a compelling case for the conceptual difference between “information” and “intelligence,” wherein the value of intelligence is epitomized in its ability not only to collect and relay information, but to analyze and interpret its meaning to the consumer.

Again, aspects of the speed versus quality challenge inherent in current intelligence hold a particular set of challenges in this regard. Current intelligence assessments require timely dissemination, thus imposing limitations to the degree of methodical analysis to which the information can be subjected. This potentially induces a problem related to expectation management (i.e., the potential discrepancy between what intelligence consumers expect and what they get). It is therefore an important precondition for productive producer–consumer relations to convey the limitations and uncertainties involved in intelligence assessments as well as providing an appropriate understanding of existing capabilities. Such understanding will ideally enhance the competence among consumers to direct questions at intelligence agencies, and cater for an optimized process of intelligence production relying on appropriately formulated problems and delegated collection.

The flipside is the need for intelligence producers to understand their consumers. An efficient and optimized intelligence process should build on a well-established mutual understanding between intelligence producers and consumers, taking into account their respective preconditions and requirements. While challenging to achieve, a productive relationship is defined by interaction and communication.

A potentially significant driver of change in the means by which intelligence agencies approach the challenges associated with information availability is the rapid evolution of AI. With its capacity for augmenting human cognition, AI is playing an increasingly prominent role in information management in general and will in all likelihood become an increasingly integrated feature of intelligence analysis. AI and ML technologies are frequently presented as the solution to the problem of processing and analyzing large amounts of information. However, these technologies also introduce new challenges that will require continuous development and adaptation on the part of intelligence agencies, if not wholesale changes in the way in which intelligence collection and analysis work is understood and conducted that are difficult to foresee. Yet, while the potential inherent in AI and ML denotes a very rapidly growing capacity for handling big data, the integration of these technologies with existing human capabilities raises issues relating to a spectrum of unresolved problems, including issues of information security, the relationship between open and secret information in intelligence analysis and, prominently, the preconditions for entrusting sensitive and potentially risky tasks to new technologies and algorithms. The introduction of new technologies also requires new skill sets among intelligence personnel, who need to develop the capacity not only to understand what these technologies are able to do, but also their limitations and the potential consequences of introducing them.

Addressing the changing dynamics of intelligence is vital as boundaries between different fields of intelligence are becoming blurred, and in the face of an increasingly complex and interconnected security environment. In this context, the significance of intelligence agencies and professionals is potentially greater than ever before, not only as collectors and disseminators of vital information, but as gatekeepers and interpreters capable of identifying the significant and consequential in a constantly multiplying volume of irrelevance. Although this article has primarily been concerned with concrete implications of the information environment for current intelligence work, these implications and the challenges they reflect relate directly to the larger task of ensuring that intelligence is adapted and utilized to its full potential.

DISCLOSURE STATEMENT

The authors report there are no competing interests to declare.

REFERENCES

- ¹ Amy Zegart, "Open Secrets: Ukraine and the Next Intelligence Revolution," *Foreign Affairs*, Vol. 102, No. 1 (2023), p. 64.

- ² Richard Shultz, “Post-9/11 Wartime Intelligence Analysis,” *Intelligence and National Security*, Vol. 33, No. 7 (2018). doi:10.1080/02684527.2018.1489998
- ³ James L. Regens, “Augmenting Human Cognition to Enhance Strategic, Operational, and Tactical Intelligence,” *Intelligence and National Security*, Vol. 34, No. 5 (2019). doi:10.1080/02684527.2019.1579410
- ⁴ See, for example, Samuel C. Woolley and Philip N. Howard, *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (New York: Oxford University Press, 2019). This edited volume includes chapters on Ukraine, Canada, Poland, Taiwan, Brazil, Germany, the United States, and China, where computerized propaganda has been used to manipulate political discourse and shape public opinion.
- ⁵ Randolph H. Pherson, Penelope Mort Ranta, and Casey Cannon, “Strategies for Combating the Scourge of Digital Disinformation,” *International Journal of Intelligence and CounterIntelligence*, Vol. 34, No. 2 (2021). doi:10.1080/08850607.2020.1789425
- ⁶ As outlined by Stottlemire, “To be considered intelligence collection, the collector’s intent must be to amass information for use by national security decisionmakers [or other consumers]. To be considered OSINT collection, the collector must acquire information second hand—that is, acquire information that was not originally provided to specifically support national security objectives. To be considered HUMINT, collectors must secretly elicit information that satisfies intelligence questions issued to the collector. See Steven A. Stottlemire, “HUMINT, OSINT, or Something New? Defining Crowdsourced Intelligence,” *International Journal of Intelligence and CounterIntelligence*, Vol. 28, No. 3 (2015). doi:10.1080/08850607.2015.992760
- ⁷ David Omand, Jamie Bartlett, and Carl Miller, “Introducing Social Media Intelligence (SOCMINT),” *Intelligence and National Security*, Vol. 27, No. 6 (2012). doi:10.1080/02684527.2012.716965. They add that two important tests need to be passed to include SOCMINT: “that it rests on solid methodological bedrock of collection, evidence, verification, understanding and application ... [and] that the moral hazard it entails can be legitimately managed.”
- ⁸ David Omand, “Spy Time: The Hunt for Chronophages,” *Intelligence and National Security*, Vol. 36, No. 5 (2021). doi:10.1080/02684527.2021.1882807
- ⁹ Alan Breakspear, “A New Definition of Intelligence,” *Intelligence and National Security*, Vol. 28, No. 5 (2013). doi:10.1080/02684527.2012.699285
- ¹⁰ John A. Gentry and Joseph S. Gordon, *Strategic Warning Intelligence: History, Challenges, and Prospects* (Washington, DC: Georgetown University Press, 2019), p. 12, citing Kevin P. Stack, “Competitive Intelligence,” *Intelligence and National Security*, Vol. 13, No. 4 (1998). doi:10.1080/02684529808432511; John W. Bodnar, *Warning Analysis for the Information Age: Rethinking the Intelligence Process* (Washington, DC: Joint Military Intelligence College Center for Strategic Intelligence Research, 2003); Arthur S. Hulnick, “The Intelligence Producer—Policy Consumer Linkage: A Theoretical Approach,” *Intelligence and National Security*, Vol. 1, No. 2 (1986). doi:10.1080/02684528608431850

- ¹¹ Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*, 6th ed. (Thousand Oaks, CA: CQ Press, 2020).
- ¹² Michael Brecher, *Crises in World Politics: Theory and Reality* (New York: Pergamon Press, 1993); Jakob Gustavsson, *The Politics of Foreign Policy Change: Explaining the Swedish Reorientation on EC membership* (Lund: Lund University Press, 1998); Richard N. Lebow, *Between Peace and War: The Nature of International Crisis* (Baltimore: Johns Hopkins University Press, 1981).
- ¹³ Arjen Boin, Paul 't Hart, Eric Stern, and Bengt Sundelius, *The Politics of Crisis Management: Public Leadership Under Pressure*, 2nd ed. (Cambridge, UK: Cambridge University Press, 2017), pp. 6–7; John T. Keeler, “Opening the Window for Reform: Mandates, Crises, and Extraordinary Policymaking,” *Comparative Political Studies*, Vol. 25, No. 4 (1993). doi:10.1177/0010414093025004002
- ¹⁴ John A. Gentry, “Intelligence in War: How Important is it? How Do We Know?,” *Intelligence and National Security*, Vol. 34, No. 6 (2019). doi:10.1080/02684527.2019.1611205
- ¹⁵ William E. Odom, “Intelligence Analysis,” *Intelligence and National Security*, Vol. 23, No. 3 (2008). doi:10.1080/02684520802121216
- ¹⁶ Joshua Rovner, “Intelligence in the Twitter Age,” *International Journal of Intelligence and CounterIntelligence*, Vol. 26, No. 2 (2013). doi:10.1080/08850607.2013.757996
- ¹⁷ See Stevyn D. Gibson, “Exploring the Role and Value of Open Source Intelligence,” in *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities*, edited by Christopher Hobbs, Matthew Moran, and Daniel Salisbury (London: Palgrave Macmillan, 2014), pp. 9–23 for an overview.
- ¹⁸ Bowman H. Miller, “Open Source Intelligence (OSINT): An Oxymoron?,” *International Journal of Intelligence and CounterIntelligence*, Vol. 31, No. 4 (2018). doi:10.1080/08850607.2018.1492826; Gašper Hribar, Iztok Podbregar, and Teodora Ivanuša, “OSINT: A ‘Grey Zone’?,” *International Journal of Intelligence and CounterIntelligence*, Vol. 27, No. 3 (2014). doi:10.1080/08850607.2014.900295; Arthur S. Hulnick, “The Downside of Open Source Intelligence,” *International Journal of Intelligence and CounterIntelligence*, Vol. 15, No. 4 (2002). doi:10.1080/08850600290101767; Joseph M. Hatfield, “There Is No Such Thing as Open Source Intelligence,” *International Journal of Intelligence and CounterIntelligence* (2023). doi:10.1080/08850607.2023.2172367
- ¹⁹ Interview, former senior official, extensive experience from senior positions in a number of U.S. government agencies, May 2022. This tendency has also been observed by the authors in their discussion with intelligence officials and in different closed-door workshops. See also Tore Pedersen and Pia T. Jansen, “Seduced by Secrecy—Perplexed by Complexity: Effects of Secret vs Open-Source on Intelligence Credibility and Analytic Confidence,” *Intelligence and National Security*, Vol. 34, No. 6 (2019). doi:10.1080/02684527.2019.1628453.
- ²⁰ Interview, former senior UK official, spring 2022.
- ²¹ *Ibid.*

- ²² Interview, former senior U.S. official, spring 2022.
- ²³ Interviews, Western Europe and the United States, spring 2022.
- ²⁴ Interview, former senior UK official, spring 2022.
- ²⁵ Mark M. Lowenthal, “Intelligence is NOT About ‘Telling Truth to Power,’” *International Journal of Intelligence and CounterIntelligence*, Vol. 34, no. 4 (2021). doi:10.1080/08850607.2021.1928438
- ²⁶ Interview, former senior UK official, spring 2022.
- ²⁷ *Ibid.*
- ²⁸ This pattern has been streaming through all our interviews. Interviews with former and current intelligence staff, spring 2022.
- ²⁹ *Ibid.*
- ³⁰ Interviews with former and current intelligence staff, spring 2022.
- ³¹ Interview, spring 2022.
- ³² Niklas Nilsson, Mikael Weissmann, and Björn Palmertz, “Hybrid Threats and the Intelligence Community: Priming for a Volatile Age,” *International Journal of Intelligence and CounterIntelligence* (forthcoming).
- ³³ Interview, spring 2022.
- ³⁴ Interview, former senior U.S. official, spring 2022.
- ³⁵ Cf. Gregory F. Treverton, “Theory and Practice,” *Intelligence and National Security*, Vol. 33, No. 4 (2018). doi:10.1080/02684527.2018.1452596
- ³⁶ Interview, former senior U.S. official, spring 2022.
- ³⁷ *Ibid.*
- ³⁸ *Ibid.*
- ³⁹ Interview, former Swedish official, summer 2022.
- ⁴⁰ Interview, former senior UK official, spring 2022.
- ⁴¹ John A. Gentry, “The Intelligence of Fear,” *Intelligence and National Security*, Vol. 32, No. 1 (2017). doi:10.1080/02684527.2016.1199348
- ⁴² Interview, former senior U.S. official, spring 2022.
- ⁴³ Kelley M. Saylor, *Emerging Military Technologies: Background and Issues for Congress* (Washington, DC: Congressional Research Service, R464582020), p. 3.
- ⁴⁴ Interview, former senior UK officials, spring 2022.
- ⁴⁵ Interview, former senior U.S. official, spring 2022.
- ⁴⁶ Interview, former senior U.S. official, spring 2022.

FUNDING

This research was funded by a grant from the Swedish Armed Forces (FoT, “Forskning och Teknik,” 2022, 2023).