International Journal of Intelligence and CounterIntelligence

ISSN: (Print) (Online) Journal homepage: www.tandfonline.com/journals/ujic20

Can Private Sector Intelligence Benefit from U.S. Intelligence Community Analytic Standards?

Dorothea Gioe, Jeremey Parkhurst & David V. Gioe

To cite this article: Dorothea Gioe, Jeremey Parkhurst & David V. Gioe (2024) Can Private Sector Intelligence Benefit from U.S. Intelligence Community Analytic Standards?, International Journal of Intelligence and CounterIntelligence, 37:4, 1145-1163, DOI: 10.1080/08850607.2023.2235078

To link to this article: https://doi.org/10.1080/08850607.2023.2235078

Published online: 14 Aug 2023.

International Journal of Intelligence and CounterIntelligence, 37: 1145–1163, 2024
ISSN: 0885-0607 print/1521-0561 online
DOI: 10.1080/08850607.2023.2235078

Routledge
Taylor & Francis Group

DOROTHEA GIOE, JEREMEY PARKHURST, AND DAVID V. GIOE

Can Private Sector Intelligence Benefit from U.S. Intelligence Community Analytic Standards?

Dorothea Gioe is the Director of Training for Emergent Risk International and a Visiting Fellow with King's College London's Intelligence and Security Center. She has over two decades of experience as an operator, analyst, and manager in the U.S. Intelligence Community, commercial security sector, and the realm of leadership development. She previously served as a senior intelligence analyst for U.S. Africa Command and as a collection management officer for the Central Intelligence Agency. Thea holds an MA in Arab Studies from Georgetown University and a BA from American University, with degrees in International Relations and Peace and Conflict Resolution.

Jeremey Parkhurst spent 20 years in the U.S. intelligence community, including military and civilian roles with duty assignments spanning analysis and operations. On active duty as an Air Force intelligence officer, Jeremey was assigned to multiple Combatant Commands including Air Force Special Operations. Subsequently he joined the Defense Intelligence Agency. He currently works in the private sector on insider threat and intelligence issues.

David V. Gioe is a British Academy Global Professor and Visiting Professor of Intelligence and International Security in the Department of War Studies at King's College London. He is also an associate professor of history at the U.S. Military Academy at West Point and a history fellow for its Army Cyber Institute. He is Director of Studies for the Cambridge Security Initiative and is co-convener of its International Security and Intelligence Program. David is a U.S. Navy veteran, as well as a former CIA analyst and operations officer. The author can be contacted at david.gioe@kcl.ac.uk or David.gioe@westpoint.edu.

This analysis is solely that of the authors. It does not represent the views or position of any of the authors' employers, including the United States Department of Defense.

Abstract: The U.S. Director of National Intelligence (DNI)'s 2007 establishment of analytic standards in Intelligence Community Directive (ICD) 203 aided in the professionalization of the U.S. Intelligence Community (IC)'s analytical cadre, enshrining best practices across a diverse field of agencies and driving cultural shifts within and among U.S. IC agencies. Private sector intelligence analysis, although wide-ranging, finds itself in a growth period, driven by the recent pandemic; the increasing importance of environmental, social, and governance movements; and heightened geopolitical strife resulting from Russia's invasion of Ukraine and concern over China's aggressive foreign policies. To improve efficiency, objectivity, and value, private sector intelligence could benefit from adopting many of the standards set out in ICD 203, although absent a powerful referee like the DNI, training and enforcement of standards will remain a challenge.

INTRODUCTION: IN THE AFTERMATH OF CRISIS IS OPPORTUNITY FOR REFORM

In the wake of intelligence failures related to the U.S. Intelligence Community (IC)'s mis-assessment of Iraq's weapons of mass destruction (WMD) program in the run-up to the 2003 U.S. invasion of Iraq, and compounded by the previous tactical surprise of the 11 September 2001 (9/11) attacks, the U.S. IC faced unprecedented and largely justified public and political criticism, engendering corresponding executive and legislative branch commands to improve its analytical product across the IC. Perhaps no single instance served to reveal the deep-rooted challenges in the U.S. IC as Director of Central Intelligence George Tenet's overly confident comment that the intelligence underpinning the U.S. IC's assessment on the status of Iraq's WMD program was a "slam dunk."[1] Tenet's quote is emblematic of the litany of analytical errors (as distinct from collection failures) that resulted in the Bush administration being provided with what they thought was the "smoking gun" that would reasonably compel the United States to invade Iraq.[2] His comments reflected the end result of an IC subject to groupthink,[3] a lack of creativity, and an inability to properly identify key assumptions underpinning their analytic judgments.[4] In an effort to avoid a repetition of the intelligence failures that inhibited the U.S. IC from preventing 9/11, Congress called for the creation of the Office of the Director of National Intelligence (ODNI) in 2004.[5] Established in April 2005, the newly created ODNI sought to align and baseline the efforts of the U.S. IC and create new cultural norms discussed by the 2005 Iraq WMD

Commission, undertaking a series of initiatives leading to significant structural and cultural reforms within the U.S. IC. [6]

One significant outgrowth from the post-WMD review of U.S. IC intelligence practices was the ODNI's promulgation of Intelligence Community Directives (ICD). We focus in particular on ICD 203, Analytic Standards, published in 2007 and updated in 2015.[7] As former U.S. government intelligence analysts, we observed firsthand how ICD 203 made agencies accountable for adhering to standards long recognized as hallmarks of quality analysis[8] and created second- and third-order effects that improved analytic tradecraft and cadre. In this article, we seek to add to the nascent dialogue on the merits of applying analytic tradecraft in a private sector intelligence and security context. Having transitioned to leadership roles in private sector intelligence firms, we posit that adoption of ICD 203 analytic and tradecraft standards beyond government analysis would increase the accuracy and utility of the analysis private sector teams provide. We will proceed by justifying the need for improved and standardized private sector intelligence analysis, then will explore the exhortations and expectations of ICD 203, and finally we will map these onto the private sector's intelligence analysis requirements to ultimately conclude that, first, ICD 203 can indeed apply to private sector intelligence, and second, that doing so would help professionalize the diverse cadre of analysts and concomitantly improve their product. It is to examine why this might be the case to which we now turn.

WHY IS THERE A NEED FOR PRIVATE SECTOR ANALYTICAL PROFESSIONALIZATION?

Not unlike the organizational tumult and introspection after the failures of 9/11 and Iraq WMD, intelligence analysis teams in the private sector are currently undergoing a similar period of rapid transition driven by economic and operational shocks resulting from the COVID-19 pandemic; increasing environmental, social, and governance (ESG) impacts on private industry; and deepening geopolitical schisms ranging from Russia's invasion of Ukraine to deteriorating relations between the United States and China, America's largest trading partner. It's not just large multinational firms that are increasingly investing in intelligence analysis to help mitigate complex and dynamic security threat environments.[9] The past few years have demanded that successful businesses adapt—at speed—from focusing primarily on tactical physical or cybersecurity threats, increasing executive appetites for strategic analysis that explores threats to supply chains, labor availability, and resiliency in the face of geopolitical or regulatory shifts. This demand signal has been reflected in the (r)evolution many intelligence and security teams are undergoing, including tasking primarily tactical physical security monitoring units to expand their scope to include longer-range analysis,

standing up new strategic intelligence units, adding new analysis positions to support business units, and outsourcing strategic intelligence functions to third-party vendors of subscription and bespoke analysis. Although the scale of intelligence analytic teams is generally smaller in the private sector than the public, they must still understand their consumers and create tailored, evidence-based, and well-sourced analysis to meet consumer requirements.

As the Harvard Intelligence Project's Maria Robson Morrow has rightly observed, the private sector intelligence industry has boomed in the last decade, leading to a great diversity of terminology, mission, and tradecraft.[10] The outpouring of open-source intelligence (OSINT) responses to Russia's invasion of Ukraine revealed just how widespread and diverse these skills, and standards, have become.[11] As with the U.S. IC, there is a spectrum of private sector intelligence analysis capability and focus. Some are for-profit intelligence vendors dedicated to providing intelligence analysis to other public and private sector clients, while other companies have created internal intelligence teams, sometimes consisting of one or two individuals, solely focused on meeting company intelligence requirements. These teams have a range of analytic training and experience, with an increasing number of new hires coming directly into the private sector intelligence domain without prior government experience—although many of the teams have former U.S. IC practitioners with varying degrees of knowledge of analytic standards, leaving it up to individual organizations to determine appropriate training for their professionals on analytic tradecraft.

Prior to ICD 203, it would be fair to assess that U.S. IC analytic tradecraft was more art than science and there was not an IC-wide consensus for what "good" analysis looked like. Despite the efforts by intelligence analysis pioneers like Sherman Kent and Richards Heuer, Jr. to professionalize the craft, neither was able to achieve an IC-wide codification of standards, leaving a great deal of variation within and among U.S. IC agencies—much like the differences that exist between private sector intelligence and security organizations today. Professor emeritus at the U.S. National Intelligence University Jim Marchio laid out several analytic standards recognized by leaders within the U.S. IC since the inception of the field, which were incorporated into ICD 203 in 2007. Marchio claims that the application of these standards was intermittent due in part to the competition for space in products that were becoming ever shorter in response to consumer demand.[12] This is a challenge that also frequently constrains private sector intelligence analysis, as it does their government counterparts, where time-pressed executives expect the intelligence picture, strategic as well as tactical, to be as brief and easily digestible as reports coming from other business functions, where, unlike inherently uncertain intelligence, sales figures, units shipped, or price to earnings ratios may be easier to grasp with confidence.

Compounding this challenge is that private sector business intelligence consumers span the spectrum of exposure to intelligence tradecraft, with some having little to no appreciation of the elements of tradecraft that distinguish between higher- and lower-quality products. Such instances risk both underutilization of intelligence as well as corporate inefficiency, leaving executives and the analysts they hire reliant on each other to determine the methodologies or standards by which corporate intelligence should be gathered, analyzed, and packaged—absent any industry-wide accepted norms to help guide them.

WHAT DOES ICD 203 REQUIRE? WHAT DOES IT OFFER?

With the publication of ICD 203, Analytic Standards, the ODNI attempted to align IC production and make U.S. IC agencies accountable to craft analysis that is:

1. objective,
2. independent of political consideration,
3. timely,
4. based on all available sources of intelligence information, and
5. implements and exhibits nine Analytic Tradecraft Standards (addressed separately below; Figure 1).

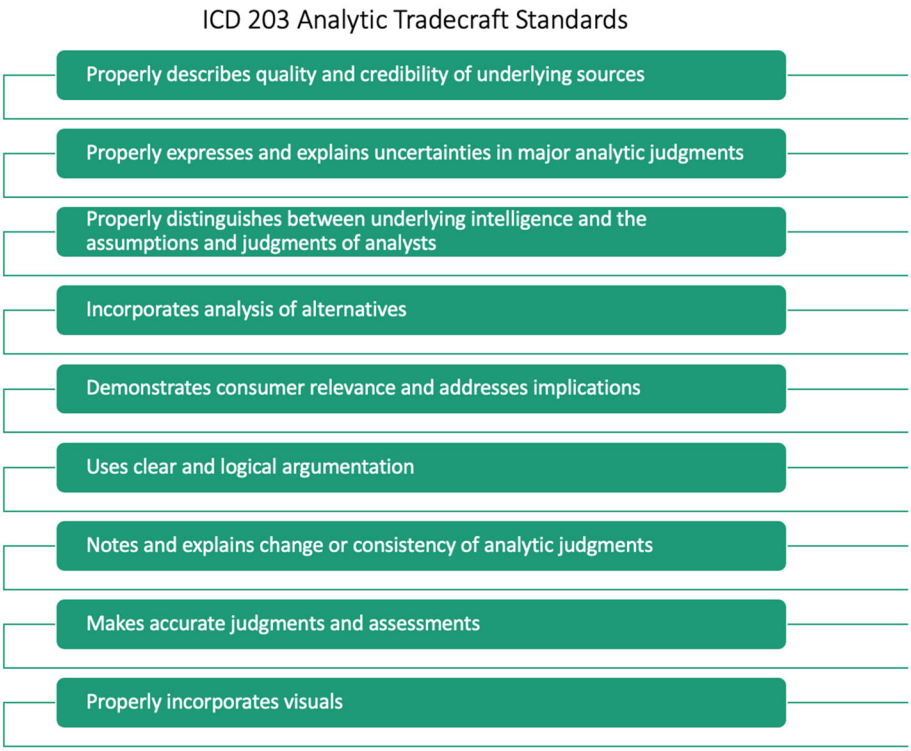

Figure 1. Intelligence analysis tradecraft standards.

Canadian researchers Hendriks and Mandel, looking at the applicability of U.S. IC analytic standards to Canadian IC intelligence production, concluded, "ICD 203 scales may serve as a useful, low-cost source of information for promoting situational awareness and accountability in intelligence organizations." We posit this is equally true in the private or public sector, based on our experiences working in both.[13] Former ODNI Deputy Neil Wiley furthered that ICD 203 came to embody an ethical standard for intelligence analysis while also providing the techniques and procedures to help codify this ethic into a tangible outcome.[14] There is nothing in Wiley's thinking that would preclude application of his findings to private sector intelligence analysis and much that would benefit corporate intelligence and security team performance. As such, we examine each of the analytic standards and their corporate applicability in greater detail below.

Objectivity

Objectivity is equally valuable in the private and public sectors as one-sided or biased judgments expose decisionmakers to faulty logic that can lead to poorly considered courses of action, leaving companies and governments alike open to unwelcome (or "surprise") outcomes for which they were unprepared. For example, the Government Accountability Office documented that the U.S. Air Force did not follow best practices that included analyzing alternatives and using confidence levels in their selection process for the Space Force Headquarters, opening it to multiple claims it did not objectively make a selection.[15] Relatively few companies have set standards to help achieve objectivity, lacking codified practices for information validation and verification that force analysts to confront their own biases and cognitive dissonance as well as those in their source material in the name of expediency. Given Pew Research Center data from 2014[16] and 2020[17] that indicates U.S. consumers increasingly perceive U.S. media as biased toward either a conservative or liberal perspective, analysts must strive to acknowledge and mitigate bias in the sources on which they draw, which in the private sector often relies heavily on press reporting. This risks understanding only half of the issue and potentially alienating corporate stakeholders who may immediately discredit analysis that references only information from news outlets they perceive as mouthpieces for the "other side." This could be a particular corporate problem, as governments have vastly more resources to spend on their own intelligence collection mechanisms. Corporations rely more heavily on publicly available and nongovernmental data (largely legacy media), which actually bolsters the case for a designated and recognized set of analytical standards.

Independence from Political Considerations

When ICD 203 stated analysis should be "independent of political consideration," it was, of course, referring to the political affiliations of executive and legislative branch leaders and not the C-suite; however, private sector practitioners can be just as subject to influence to provide information that aligns to a senior leader's desired message and bottom-line forecasts. For example, leadership may take issue with cyberintelligence professionals discussing weaknesses in software developed by a company with which there may be a preexisting partnership or potential financial arrangement. Similarly, teams that point out risks that arise from supply chain relationships with countries perceived as hostile, that fail to uphold human rights or meet environmental standards, may encounter pushback from executives who would rather these issues not be aired even internally. ICD 203 has clarified and codified this within the public sector, but the appreciation of this standard varies among private sector intelligence shops and may be entirely absent at senior executive levels, where exposure to public sector intelligence may be limited to Hollywood depictions. Acceptance of this as a best practice for intelligence analysts, regardless of sector, would eventually result in clearer expectations of the role of private sector analysts—both for themselves and their employers.

Further, with no federal legal framework in the United States to protect workers from discrimination based on political affiliation, intelligence analysts may rightly think twice before "speaking truth to power," as this ICD standard is frequently interpreted by public sector analysts. As politics around the globe have become more polarized over the last decade,[18] political viewpoints have increasingly colored corporate cultures and board room decisions,[19] resulting in corporate atmospheres where it is obvious to those working there what is the "correct" answer. Combined with increasingly partisan open-source reporting, not to mention the proliferation of mis- and disinformation along political narratives,[20] analysts operating without articulated standards may perceive from their corporate culture that there are preferred media outlets from which they should be drawing.

Political considerations may be international as well as domestic, as private sector analysts who must contend with organizations fearful of political blowback to their bottom line can attest. China is not the only nation willing to cut off business as retaliation for commentary perceived as critical of its political, military, economic, legal, or cyber activity, although with many multinationals establishing facilities across China as they vie for market share, it is certainly one of the most obvious. The National Basketball Association felt the sting of Chinese retribution in 2019 following a pro–Hong Kong tweet from the Houston Rockets general manager,[21] and Hollywood has been repeatedly criticized for pandering to Chinese audiences,

avoiding references to Hong Kong, Taiwan, Xinjiang, or other politically sensitive areas. This desire to shield company profits can directly or indirectly influence analytic products from providing a comprehensive and thorough intelligence product that attributes nefarious activity or heightened financial or operational risks to a nation-state.

Timeliness

Timeliness is critical in the field of intelligence analysis, whether public sector or private, although the expectations of what constitutes timeliness may vary considerably between the two realms, especially since the U.S. IC is often supporting military personnel in combat environments. Nevertheless, while "timely" in the IC can mean weeks or months for the production of IC-coordinated analysis, in the private sector, analysts are frequently required to turn around a finished product in a matter of days and sometimes hours. This compressed timeline has obvious implications for how analysts can conduct their work, including limiting the opportunity to apply many structured analytic techniques (SATs) that may occupy multiple team members for hours, or to coordinate with stakeholders who are not immediately available. However, timeliness can also suffer from the second-order effect of companies striving to shield themselves from political or legal liability through extra, artificially induced review processes that can inhibit intelligence production that is timely and therefore relevant. Or worse, absent a professional set of standards, what is to prevent a company from obstructing intelligence production that might expose existing regulatory, legal, or brand risks, as certain oil and gas companies previously prevented their scientists from publishing data confirming the links between hydrocarbon emissions and climate change?[22]

All Available Sources of Intelligence Information

The analytic standard that exhorts intelligence analysts to use "all available sources of intelligence information" refers to the totality of the enormous volume of information available to IC analysts. ICD 203 laid out this standard to guard against stove piping of information and the groupthink that can promote. The concept underpinning this statement is that analysts should include conflicting information to provide a more nuanced and honest product to their clients. Intelligence analysts do not wish to make the choices for their consumers, but rather to make their choices as clear as possible. This concept is equally applicable to private sector practitioners, although many junior analysts fear providing conflicting information, falsely believing it undermines their report or proposed action. Correspondingly, leaders can either intentionally (through the inculcation of a politicized work

environment) or unintentionally (through tight deadlines or overtasking of a limited team with variable tradecraft experience) contribute to an environment where their team members are reticent to provide conflicting information, thereby creating knowledge gaps and blind spots.

Without an identified and agreed on analytic standard, many of these teams struggle with how to access, evaluate, and integrate a variety of credible sources (as opposed to highly politicized content or even misinformation) into a comprehensive product, not to mention how to leverage the unique skills of the various team members to create the best possible product with the greatest efficiency. However, research from Marcoci et al. on the assumptions underpinning the rollout of ICD 203 found that the "standard of good reasoning" present across the U.S. IC due to the rollout of ICD 203 was "more reliable and valid than implied by its critics."[23] However, it should be noted that Marcoci et al. also found the requirement for all new analysts to go through a common basic training course on these standards was likely seminal to the manifestation of these benefits; that is, the adoption of standards alone may be insufficient to yield a noticeable improvement in analysis but can serve as an essential first step.

WOULD THE ICD 203 SLIPPER FIT THE PRIVATE SECTOR PRINCESS?

While not all nine tradecraft standards enumerated in ICD 203 need appear in the final analytic product targeted at the business consumer, integration of (and training on) this tradecraft at the working level has direct value for private sector analysts. In our experience, many corporate intelligence teams individually fail to apply more than a couple of these consistently, and across the broad field of private sector intel—which as we have noted ranges vastly in size and remit from organization to organization—there is little discussion, let alone agreement, regarding the relative merits of these standards. While public sector intelligence consumers, especially veteran diplomats, policy wonks, and senior military officers, have some expertise in the world of intelligence, private sector consumers of intelligence often lack a full understanding of what intelligence can offer them and, as such, are not fully reaping the benefits of what insights intelligence can provide to them, much less externally driving analytical standards. Analytic teams themselves, as noted previously, increasingly come from a variety of backgrounds and experiences where exposure to ICD 203 standards is anything but assured. Below, we address the role these nine standards can play in the private sector and assess which have the most immediate relevance to the broad field of private sector intelligence analysis.

The first two standards laid out in ICD 203, "properly describes quality and credibility of underlying sources" and "properly expresses and explains uncertainties associated with major analytic judgments" are perhaps the two

least likely to see widespread adoption in finished private sector intelligence. This is driven by two key factors, both rooted in the consumer's needs and expectations. The first is time and the second is level of interest. The higher the executive, the less time they have available to ingest intelligence to aid decisionmaking. They want the bottom-line up front: the most salient analysis backed by the most relevant facts. At the C-suite level, these consumers have neither the time nor the interest in the details that went into "sausage making." While this lack of prioritization of intelligence products may be regrettable—and even unwise—from the perspectives of those who produce intelligence precisely to aid decisionmaking, it is a phenomenon that we have observed across public and private sectors. As such, expressing the limits of what is known and the possibilities of what is unknown is often the first thing to get cut from urgent analytical updates, no matter the context.

Rarely in private sector intelligence does the finished product—often a streamlined page or two or perhaps an interactive data-driven online dashboard—address the quality and credibility of sources, incorporate alternative views, or detail uncertainties behind analytic judgments. While source descriptions are almost never requested by corporate clients (unless there is a significant concern on the veracity of key information) in favor of succinct analysis focused on key judgments, ensuring analytic teams understand and can speak to the totality and quality of evidence on analysis represents a maturation opportunity as intelligence professionals. Similarly, the level of coordination and creation of space for differences of perspective is something beyond the scope of all but the largest teams of corporate intelligence analysis. Inclusion of uncertainties—or, for instance, including a dissenting or "red team" opinion from a team member—would, in many instances, be seen as counterproductive by corporate executives and clients who pay intelligence analysts to provide expertise on the world of risks and threats (i.e., to have taken all that into consideration before laying out the bottom line). Corporate teams that vary in their opinions about likely trajectories or events unfolding too rapidly to pin down a single likely outcome find it more useful to lay out scenarios with separate indicators and warnings, enabling executives and clients to contemplate a variety of mitigation plans rather than lay their intellectual arguments before a chief executive like a high judge. This, in our view, harkens back to the epistemic basis of intelligence: not to forecast the future, but to narrow the cone of uncertainty for the decisionmaker.

Having worked with several intelligence teams across various contexts, we submit that several already effectively employ the third tradecraft standard, "properly distinguishes between underlying intelligence and the assumptions and judgments of analysts." In the U.S. IC, this is often done by putting assessments in bold italics, immediately followed by the evidence that

supports it, a technique that has carried over to some private sector teams, likely brought by a former U.S. IC member who had a hand in starting up corporate intelligence product lines. Other organizations favor putting analysis in one color and evidence in black text or putting analysis in a box with the evidence underneath. These measures are often employed by teams that also value putting the analysis up front, understanding that insight—not research—is the true value they add for their consumer. This offers the added benefit of training the consumer to expect the analysis in the same place on the page, easing ingestion of the key takeaways.

With respect to incorporating analysis of alternatives (AoA), many private sector analytic teams are reticent to incorporate this fourth tradecraft standard for the same reasons they are averse to including analytic dissent, as discussed above. In this case, there is also concern incorporation of AoA weakens the overall intelligence product or will cause executives to doubt the corresponding analytic judgments. In actuality, conveying unknowns inherent in intelligence strengthens the argument and fosters a more authentic relationship between the intelligence practitioner and their client. Incorporating AoA, or other SATs—such as using indicators and warnings, structured brainstorming or scenarios-based analysis—can allow intelligence products to better mitigate potential strategic surprise and increase objectivity, although this remains an area ripe for additional research.[24] However, smaller private sector intelligence analysis teams may lack the depth of expertise or personnel to effectively incorporate SATs, while larger teams may need additional training to enable analysts from diverse professional backgrounds to apply these techniques soundly.

Highly successful private sector teams already "demonstrate consumer relevance and address implications and use clear and logical argumentation." They address business implications of the issues they are tracking based not only on their knowledge of the issues or events but of their business and its value chain. Using clear and logical argumentation, they make accurate judgments and assessments, leading with the most impactful insights that will aid time-strapped executives and clients. The proliferation and expansion of private sector intelligence teams and their remits accelerated during the COVID-19 pandemic and have continued amid the geopolitical tensions of 2022 and 2023, indicating that teams are consistently able to demonstrate value to their employers through relevant, clear, and logical presentation of the potential impacts to business. However, as more organizations seek to expand their in-house capabilities, frequently leveraging underutilized physical security personnel to track more complex and longer-range types of risk—such as regulatory, legal, financial, or reputational risk—there will be increased need to train employees to understand how to consider the full range of business implications and hone their writing and logic skills.

Regarding the imperative to craft intelligence assessments which "[n]ote and explain change or consistency of analytic judgments," incorporating guidance to note and explain changes or consistency of analytic judgments represents a significant departure for many private sector intelligence teams, especially those without long-term baseline knowledge, such as firms which are entering new markets, or, on the other hand, firms perhaps too comfortable in a dynamic security environment. Within the U.S. IC, there is the Library of National Intelligence,[25] a repository of meta-tagged U.S. IC production that is retrievable and discoverable by analysts. There is also the concept of a standing analytic line: the totality of a department or agency's previous analytic production represents a reference point to which all new analytic production can be anchored (in both the helpful as well as the biased connotations of that word). This provides context that is often missing in private sector analysis. When a private sector intelligence product discusses a new cyber intrusion set, for example, it often fails to provide key context, especially one that goes back more than a few years. A more quotidian example would be a 10:00 AM weather report simply stating that the weather is 15 degrees Celsius without explaining why the current temperature is 15 degrees, what the weather will be seven hours later, and if the current weather is aligned to normal standards. Is 15 degrees a marked change from the average weather? Perhaps 15 degrees is a complete aberration from normal weather that time of year and represents a marked shift from "normal" weather. An ability to reference what is "normal" helps guard against what Jared Diamond labeled "landscape amnesia,"[26] incremental changes that are so gradual they are nearly imperceptible unless referenced to previous information. An easily understood example is the use of historical and current pictures to display the decrease in glacier sizes due to climate change. Although few, if any, intelligence units catalog and reference previous intelligence production, it behooves analysts to understand their previous production can serve as a reference point for their clients and that current events are better understood when the context is provided, something that can occur when the new product details how this is a change from or continuation of previous analytic judgments.

Less mature intelligence units often do not understand how to clearly convey likelihood- and confidence-level terms and ensure there is no contradiction with the assessment, mistakenly understanding "[m]akes accurate judgments and assessments" as referring to the accuracy of the assessment(s) the intelligence analyst is discussing in their product. For accuracy, ICD 203 refers to an alignment of confidence and likelihood terms with the assessment. More mature teams may provide a table or reference appendix explaining likelihood and confidence terms either qualitatively, quantitatively, or a combination of both. This can help develop consumer trust in team assessments by making it easier for busy executives to scan and

process the grades their intelligence team has assigned. However, this can also lead to a false sense of security or overconfidence.

Regarding the final tradecraft standard, private sector intelligence groups may actually be setting the bar for their public sector counterparts when it comes to properly incorporating visuals. Thanks to an ever-growing quantity of open source and proprietary data to inform and support their judgments, and a proliferation of open-source data visualization tools and software programs, private sector teams increasingly relying on visual dashboards rather pages of text to interactively inform their consumers under the old adage that a picture is worth a thousand words. It is common for teams to include maps, bar and line graphs, and other visualizations to add context to even short-form analytic products, recognizing the value of the engagement-factor. As today's younger professionals, who are more likely to turn to social media as their primary news source, move up corporate ladders, the expectation that intelligence will be short, digestible, and visually engaging will only increase.[27]

STANDARDIZATION OF ANALYTIC TRADECRAFT OFFERS LONGER-TERM CULTURAL BENEFITS

That ICD 203 can be useful outside of government corridors is an increasingly accepted view. Indeed, an initial exploration of the benefits across the private sector was raised at the Government-Private Sector Analytic Tradecraft Standards 2020 Conference.[28] It stands to reason that when practiced *en masse* by analysts, analytic standards can create a new culture where the baseline expectation is to purposely strive for objectivity and relevance while also examining one's argumentation in a comprehensive and repeatable manner. These practices foster what psychologist Daniel Kahneman called "System 2" thinking, which is slow, deliberate, and more logical.[29] Combining System 2 thinking with an organizational mandate to consider conflicting information and alternative analysis is a natural levee against bias and epistemological cocoons. We submit that this organizational encouragement of this slow, methodical thinking improves the IC analytic cadre, whether that be at an analyst or leadership level. These basic principles are well served by but can also be easily transferred to consultants and other private sector professionals for a range of benefits.

In addition to much-needed post-Iraq invasion analytical improvements, the implementation of ICD 203 tradecraft standards was also a broader agent for cultural changes across the IC. The Iraq WMD Commission stated, "We need an Intelligence Community that is truly integrated, far more imaginative and willing to run risks, open to a new generation of Americans and receptive to new technology."[30] Thanks to the COVID-19 pandemic, ESG movement, and recent consequential geopolitical tensions, private sector

intelligence has been undergoing a similar cultural shift. This has been driven by the recognition of the critical role intelligence teams can play in insulating organizations from more than just physical threats, to including supply chain, cyber, reputation, regulatory, and financial risks, to name but a few. Moreover, are the costs organizations face when they fail to plan mitigation measures properly in the face of these challenges.

What remains to be seen is whether these cultural changes will remain the new norm, but ICD 203 is at least a step in the right direction, and it can help solidify both tradecraft and cultural improvements. However, one critique of public sector intelligence adoption of these standards includes the potential for a senior intelligence official to force a top-heavy and duplicative review process, or even go so far as to needlessly insert themselves in routine analytic tasks, since all this accomplishes is the professional stunting of mid-level and junior analysts, in contradiction to the spirit of ICD 203.

From a private sector perspective, the absence of clearly defined analytic standards would not, in and of itself, prevent the potential for such aggressive managerial review, as analysts remain subject to the whims of leadership that could also contribute to the analytic flaws Marchio observed in 2014 and that are still commonplace nearly a decade later among private sector intelligence practitioners. One would need to look no further than the current corporate emphasis on "getting back to normal," despite the identified benefits of forced cultural and process changes that were necessitated by the pandemic.

A more robust and clearly defined analytical contribution to the private sector could also help analysts demonstrate added value—over a certain baseline—within the corporate entities. Talk of cuts in the private sector intelligence workforce seems to ape neatly economic downturns, especially as companies are struggling in an environment of heightened uncertainty regarding supply chains, energy supplies and regulations, sanctions regimes, and often political risk. While intelligence is usually seen as a necessary cost in the private sector, it is not implausible that cuts may be based, at least in part, due to the perceived inefficacy of the teams. Such thinking raises the rather obvious question of whether the perceived value those teams might have added would have been improved by applying strengthened analytic standards, which would have the added benefit of sensitizing corporate consumers to the added value of rigorous analytic tradecraft. Although the benefits of, and corresponding justification for, an effective intelligence unit for companies are increasingly documented by individuals such as long-service public and private sector intelligence veteran Paul R. Kolbe, their adoption is not universal, nor is the understanding of the decision dominance they can provide.[31] Much work remains to be done both in changing corporate culture and evangelizing analytical value added in the C-suite, but ICD 203 is the proper foundation on which to build.

We recognize that there is no forcing function for private sector professionals as there is within the U.S. IC, namely the DNI, and this, in turn, requires adoption based on value-added instead of DNI fiat. Although a few private sector intelligence associations already exist to improve analysis in the private sector (such as the Association of Intelligence Risk Professionals), there is no industry-wide consensus on best practices. The August 2022 launch of the OSINT Foundation—a group of former U.S. IC officers intent on bringing community-wide standards to OSINT analysts—further demonstrates the absence of higher authority with that forcing function to date.[32] However, it is unlikely that this new organization, with its vision still solidly focused on U.S. national security, will become the external catalyst for analytic standards across the multinational private sector. Instead, any successful approach must take a more confederate approach that stresses compromise, agreement, and individual accountability. An additional step worthy of consideration for firms is establishing independence and conflict of interest rules for intelligence professionals similar to what is currently established for accountants and many other journeyman trades.

Adopting a common set of analytic standards across the private sector would improve objectivity, depth of analysis, and, ultimately, the corporate bottom line. Moreover, the expansion of private sector intelligence can serve as a model for furthering the concept that the IC and private sector can effectively cross-pollinate practices of benefit to the other. We endorse the idea that increased collaboration empowers both sectors with more decisive actions in protecting both the public and individual companies. Barring an external forcing function, industry-wide training to commonly accepted standards is the most likely first step toward consistent achievement. Adopting sector-wide standards would necessitate training standards certification, which currently does not exist, although several private entities offer versions of private sector intelligence analysis training that could serve as foundational models.

Another pathway is through the use of intelligence analysis programs increasingly offered in higher education. As many students completing these programs join either public or private sector intelligence teams, this helps baseline common standards for new practitioners and sets the foundation for future leaders attuned to fostering good tradecraft. Consistent training on analytic tradecraft—whether offered by industry professionals or through academic institutions—would almost certainly result in more sophisticated intelligence teams capable of accurately applying techniques increasingly viewed as best practices no matter the context (like SATs). This could yield more nuanced assessments of the bottom line and offer insights to help hedge against the most likely outcome as well as lower likelihood but potentially high-impact futures.

The adoption of standards, training, and certification thereof are steps that would surely also need to be accompanied by mechanisms to censure those who stray from those practices, either individually or organizationally, which is another area for future research and development.[33] It can also help foster intelligence teams that better anticipate threats and identify trends and opportunities. As Kolbe and Morrow have documented, there is a growing body of private sector firms utilizing intelligence to proactively address and therefore avoid longer-term risks.[34] Common standards within the private sector could also further existing U.S. IC–private sector collaboration, helping to create more common language and standards while also complementing existing outreach such as the Department of Homeland Security Public-Private Analytic Exchange Program[35] or the Overseas Security Advisory Council.

CONCLUSION

As we have argued in this article, the adoption of analytical tradecraft standards based on those laid out in ICD 203 can indeed apply to the private sector analytical effort and would go far in ensuring analysts representing a diversity of professional and experiential backgrounds (and their products) can be harnessed to provide improved products and increase value, including future-proofing analytical efforts that can evolve with technology and in response to unforeseen circumstances. Although significant differences exist between the IC and private sector, ICD 203 standards can be adopted and tailored accordingly to foster positive communication and understanding between analysts and corporate decisionmakers.

REFERENCES

[1] Huw Dylan, David V. Gioe, and Michael S. Goodman, *The CIA and the Pursuit of Security* (Edinburgh: Edinburgh University Press, 2020), p. 427.
[2] Wolf Blitzer, "Search for the Smoking Gun," *CNN*, last modified 10 January 2003, https://www.cnn.com/2003/US/01/10/wbr.smoking.gun/ (accessed 2 October 2022).
[3] Richards J. Heuer, "Limits of Intelligence Analysis," *Orbis* (Winter 2005), https://www.iwp.edu/wp-content/uploads/2019/05/20131120_HeuerLimitsofIntelligenceAnalysis.pdf (accessed 2 October 2022).
[4] U.S. Government, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (Washington, DC: GPO, 2005), https://www.govinfo.gov/content/pkg/GPO-WMD/pdf/GPO-WMD.pdf (accessed 11 June 2022).
[5] Director of National Intelligence, ODNI Factsheet, Office of the Director of National Intelligence, last modified October 2011, https://www.dni.gov/files/documents/ODNI%20Fact%20Sheet_2011.pdf (accessed 30 September 2022).

[6] Director of National Intelligence, "Intelligence Community Directives," *Office of the Director of National Intelligence*, https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives (accessed 11 June 2022); U.S. Government, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction*.

[7] Director of National Intelligence, *Intelligence Community Directive 203*, last modified 2 January 2015, https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf (accessed 11 June 2022).

[8] Jim Marchio, "Analytic Tradecraft and the Intelligence Community: Enduring Value, Intermittent Emphasis," *Intelligence and National Security*, Vol. 29, No. 2 (2014), pp. 159–183. doi:10.1080/02684527.2012.746415.

[9] Paul Kolbe, "A CEO's Guide to Intelligence: 'Not Just for Three-Letter Agencies,'" *The Cipher Brief*, last modified 9 March 2018, https://www.thecipherbrief.com/ceos-brief-guide-intelligence-not-just-three-letter-agencies (accessed 10 October 2022).

[10] Maria Robson Morrow, "Private Sector Intelligence: On the Long Path of Professionalization," *Intelligence and National Security*, Vol. 37, No. 3 (2022). doi:10.1080/02684527.2022.2029099.

[11] David V. Gioe and Ken Stolworthy, "Democratized and Declassified: The Era of Social Media War Is Here," *Engelsberg Ideas*, last modified 24 October 2022, https://engelsbergideas.com/notebook/democratised-and-declassified-the-era-of-social-media-war-is-here/ (accessed 30 October 2022). For a different view on how to consider OSINT, see Joseph M. Hatfield, "There Is No Such Thing as OSINT," *The International Journal of Intelligence and CounterIntelligence* (2023), pp. 1–22, doi:10.1080/08850607.2023.2172367.

[12] Marchio, "Analytic Tradecraft and the Intelligence Community."

[13] Tonya Hendriks and David Mandel, "Intelligence Professionals' Views on Analytic Standards and Organizational Compliance," Assessment and Communication of Uncertainty in Intelligence to Support Decision Making: Final Report of Research Task Group SAS-114 (Brussels: North Atlantic Treaty Organization Science and Technology Organization, 2019), https://ssrn.com/abstract=3433560 (accessed 10 October 2022).

[14] Neil Wiley, "Conference Report: Government-Private Sector Intelligence Tradecraft Standards," Presentation, Centra Technology, Inc., Kennan Conference Suite, Arlington, Virginia, 11 February 2020, https://cdn.ymaws.com/www.iafie.org/resource/resmgr/2019_site_misc/agenda_gov-priv_sector_analy.pdf (accessed 12 October 2022).

[15] Scott Maucione, "GAO Says Airforce Decision on SPACECOM was Sloppy," *Federal News Network*, last modified 3 June 2022, https://federalnewsnetwork.com/air-force/2022/06/gao-says-air-force-decision-on-spacecom-location-was-sloppy/ (accessed 12 October 2022).

[16] Amy Mitchell, Jeffrey Gottfried, Jocelyn Kiley, and Katerina Eva Matsa, *Political Polarization & Media Habits*, Pew Research Center, last modified 21 October 2014, https://www.pewresearch.org/journalism/2014/10/21/political-polarization-media-habits/ (accessed 20 October 2022).

[17] Mark Jurkowitz, Amy Mitchell, Elisa Shearer, and Mason Walker, *U.S. Media Polarization and the 2020 Election: A Nation Divided*, Pew Research Center, last modified 24 January 2020, https://www.pewresearch.org/journalism/2020/01/24/u-s-media-polarization-and-the-2020-election-a-nation-divided/ (accessed 20 October 2022).

[18] Pew Research Center, *Political Polarization in the American Public*, last modified 12 June 2014, https://www.pewresearch.org/politics/2014/06/12/political-polarization-in-the-american-public/ (accessed 20 October 2022).

[19] Vyacheslav Fos, Elizabeth Kempf, and Margarita Tsoutsoura, *The Political Polarization of U.S. Firms* (New York: New York University, 1 April 2022), https://as.nyu.edu/content/dam/nyu-as/econ/documents/spring_2022/Partisan%20Firms_NYU.pdf (accessed 23 October 2022).

[20] Mathias Osmundson, Michael Bang Petersen, and Alexander Bor, "How Partisan Polarization Drives the Spread of Fake News," Brookings Institution, last modified 13 May 2021, https://www.brookings.edu/techstream/how-partisan-polarization-drives-the-spread-of-fake-news/ (accessed 29 October 2022).

[21] Rosie Perper, "China and the NBA Are Coming to Blows over a Pro-Hong Kong Tweet. Here's Why," *Business Insider*, last modified 23 October 2019, https://www.businessinsider.com/nba-china-feud-timeline-daryl-morey-tweet-hong-kong-protests-2019-10?r=US&IR=T#on-october-7-democrat-and-republican-lawmakers-hit-back-over-the-nbas-shameful-response-to-chinese-backlash-7 (accessed 10 October 2022).

[22] Shannon Hall, "Exxon Knew about Climate Change almost 40 Years Ago," *Scientific American*, last modified 26 October 2015, https://www.scientificamerican.com/article/exxon-knew-about-climate-change-almost-40-years-ago/ (accessed 22 October 2022).

[23] Alexandru Marcoci, Ans Vercammen, and Mark Burgman, "ODNI as an Analytic Ombudsman: Is Intelligence Community Directive 203 Up to the Task?" *Intelligence and National Security*, Vol. 34, No. 2 (2018), pp. 205–224. doi:10.1080/02684527.2018.1546265.

[24] *Ibid.*

[25] Director of National Intelligence, *Online Intelligence Library Fosters Cooperation Among Agencies*, Office of the Director of National Intelligence, last modified 6 July 2011, https://www.dni.gov/index.php/who-we-are/organizations/ise/ise-archive/ise-news/1902-online-intelligence-library-fosters-collaboration-among-agencies (accessed 25 October 2022).

[26] Jared Diamond, *Collapse: How Societies Choose to Fail or Survive* (New York: Penguin Books, 2011).

[27] Elisa Shearer and Amy Mitchell, *News Use across Social Media Platforms in 2020,* Pew Research Center, last modified 12 January 2021, https://www.pewresearch.org/journalism/2021/01/12/news-use-across-social-media-platforms-in-2020/ (accessed 1 November 2022).

[28] "Executive Summary," Conference Report, Government-Private Sector Intelligence Tradecraft Standards, Centra Technology Inc., Kennan Conference Suite, Arlington, Virginia, 11 February 2020, https://cdn.ymaws.com/www.iafie.

org/resource/resmgr/2019_site_misc/agenda_gov-priv_sector_analy.pdf (accessed 30 October 2022).

[29] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011).

[30] U.S. Government, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.*

[31] Kolbe, "A CEO's Guide to Intelligence."

[32] Dustin Volz, "New Group to Promote Open-Source Intelligence, Seen as Vital in Ukraine War," *The Wall Street Journal*, last modified 27 July 2022, https://www.wsj.com/articles/new-group-to-promote-open-source-intelligence-seen-as-vital-in-ukraine-war-11658926800 (accessed 3 November 2022).

[33] U.S. Department of Homeland Security, *The Importance of Private Sector Intelligence Programs*, 2021 Public-Private Analytic Exchange Program, last modified 2011, https://www.dhs.gov/sites/default/files/publications/importance_to_private_sector_intelligence_programs.pdf (accessed 20 November 2022).

[34] Paul Kolbe and Maria Robson Morrow, "How Corporate Intelligence Teams Help Businesses Manage Risk," *Harvard Business Review*, last modified 4 January 2022, https://hbr.org/2022/01/how-corporate-intelligence-teams-help-businesses-manage-risk (accessed 20 November 2022).

[35] U.S. Department of Homeland Security, *The Importance of Private Sector Intelligence Programs*.

ORCID

Dorothea Gioe http://orcid.org/0009-0006-5527-2187
Jeremey Parkhurst http://orcid.org/0009-0009-2537-4635
David V. Gioe http://orcid.org/0000-0003-4310-999X