Chapter 11
Written Reports and Verbal Briefings

Bottom Line Up Front

Written reports and **verbal briefings** in security analysis are meant to both inform and persuade customers and larger audiences. There are no standard formats for these reports and briefings. There are; however, some general guidelines for preparing reports and briefings. Most intelligence reports and briefings include a title, key judgments, detailed arguments, outlooks, and implication assessments. Security policy analysis reports and briefings are similar to those in intelligence, but include recommendations and often an initial implementation plan for solving the problem under study. Once an initial draft of a report or briefing is completed, it should be submitted to a review process consisting of a structured self-critique that looks deeper at the key judgments; then, a self-review of the draft report or briefing using critical-thinking Intellectual Standards. For intelligence written reports, a more formal, external Devil's Advocacy challenge review is required.

A Different Approach

Security analysis written reports and verbal briefings likely differ from how analysts developed such material in the past. In elementary school, secondary school, and even college, most students are taught a general humanities writing approach: organize and present the information and then lead the reader or listener to a final conclusion. This is not how security analysis reports and briefings are formatted. Academics using the scientific method may prepare reports with sections for a literature review, theoretical framework, research design, hypothesis tests, analysis, findings, and conclusions. Security reports and

briefings are formatted differently than those in academia. Many of the skills learned from research and analysis at all levels in academia are important to preparing security analysis reports and briefings, such as information searching, logic employment, punctuation, spelling, grammar, sentence construction, and paragraph construction.

Similar to journalistic stories, security analysis reports are prepared with the most important material presented first; that is, by addressing *who, what, where, when,* and *how* of the situation. Later in the journalist's story, they present more detailed supporting evidence and reasoning. This journalistic formatting is due to two main factors. First, some customers will only "speed read" headlines and initial paragraphs or quickly listen to verbal story leads. Thus, the main points must be presented at the start. Busy customers often look to catchy headlines and the first few written paragraphs or lead statements of a story to "grab" their attention and convey the gist of the story—without reading or listening to the entire story. Second, editors for media written and verbal stories cut material from the bottom-up to fit existing page and column constraints or time allotted for verbal stories. Security analysis written reports and verbal briefings start with their findings followed by the evidence and reasoning that supported the findings.

There is no one format; however, for developing security analysis written reports and verbal briefings. Some will be written only, some verbal only, and some will require both written and verbal reports. Written reports range from one or two pages to hundreds of pages and may be published in a variety of locations. Verbal briefings normally focus on a single customer and related audience. Live or recorded video briefings also may be given and posted on the Internet. Written reports and verbal briefing formats will depend on the issue or development for the analysis (i.e., the questions being answered and/or problem being addressed), the primary customer or audience for the analysis, and the style guide for their home organization. Some reports and briefings, especially tactical or current-event reporting, may provide only one to three pages of written text or a few briefing slides. Other reports and briefings may take 10-20 pages of written

text or 20 or so briefing slides. Still other reports and briefings may require 50-100 pages or more of written text, but still with 20 or so briefing slides, as long verbal briefings may lose the audience.

The content and format for written reports and verbal briefings must be tailored for the customer and audience. Some customers or audiences may be new to the security field or specific event or development under analysis and may require more background and descriptive details. Other customers or audiences may be experienced and will need less descriptive details and require only the analytic insights. Many large security organizations publish a formal style guide for formatting written reports. Academic programs will use one of the standard academic style manuals (American Psychological Association, Chicago/Turabian, Modern Languages Association, etc.). Do not expect to find pre-formatted report templates where the analyst just fills in the blanks.

The analyst's ultimate challenge is to inform and persuade the customer and audience about the event or development under analysis. In their reports and briefings, analysts must persuade the readers or listeners of the efficacy of the analytic findings. The message conveyed must be simple, concrete, and credible. Having first completed a good critical-thinking analysis makes report and briefing development easier. *Reports and briefings are only prepared after the critical-thinking analysis is complete.* As the reports and briefings are in development and review, the analyst likely will find gaps in the analysis and will have to revisit one or more of the critical-thinking elements of thought. While there is no single format for preparing security analysis reports and briefings, this chapter provides general guidance for their drafting. This guidance is largely standard in the security field. This chapter also presents the process for conducting structured self-critiques, self-reviews, and challenge analyses before written reports and verbal briefings are published or presented to customers. Lastly, do not be surprised; however, if some readers or listeners initially are skeptical or even hostile toward the findings.

Getting Started: Title and BLUF

The first item anyone notices in a written report or verbal briefing is the **title**. Use the title to catch the customer or audience's attention from the start. It must also convey an analytic message,[1] by providing the "*who, what, and so what*" of the written report or verbal briefing.[2] The title must convey who the key actor(s) is/are in the analysis and should include an action verb to highlight the event or development addressed in the written report or verbal briefing. The action verb usually is followed by a few words to state the "*so what*" of the analysis; that is, indicate why it is important the reader or listener pay attention to the written report or verbal briefing. Be as specific as possible in the title without using too many words. Avoid using sub-titles or supporting clauses in titles. Also remember that the title may be the main focus of key word searches, so think about how other analysts may search to find the written reports or recorded verbal briefings. Examples of titles include:

> Weak: Assessing North Korean Nuclear Weapons Developments
> Better: North Korea Fields Nuclear Missiles with Reach to U.S. Pacific Coast
>
> Weak: Colombian Cocaine Supply Increases
> Better: Colombian Cocaine Supply May Double Illegal Drugs in the United States

At the start of the written report or verbal briefing, provide a **contention** or summary of the analytic message. The contention may be a thesis, key judgments, findings, conclusions, recommendations, or a combination of these items. *The contention is not the question(s) being answered by the analysis.* It is also not the hypotheses tested in the analysis. Placing the contention at the start of the written report or verbal briefing is referred to as providing the bottom-line-up-front or **BLUF**.[3] After a catchy title, the BLUF is the next item customers should

see in security analysis written reports or verbal briefings. Prepare the BLUF after developing the main arguments that support the contention.

BLUF statements depend on the type of written report or verbal briefing and length of the analysis. In verbal briefings, the BLUF should follow directly after the title slide. In shorter written reports, the BLUF should be in the first or second paragraph and often is included as part of the introduction. In longer written reports, the BLUF likely will be a separate initial section labeled the **Executive Summary**[4] and could run a page or two in 10- to 20-page reports or several pages in 50- to 100-page or longer reports. The executive summary is similar to an abstract in academic writing, but with a different focus of summarizing the content and contentions of the entire report in a short space for busy customers.

Box 11.1 provides an example of a short BLUF excerpt from the introduction to Congressional testimony by the Director of National Intelligence on the 2018 "Worldwide Threat Assessment." Examples of longer BLUF statements, normally in executive summaries, may be accessed by reviewing studies published by the U.S. Government Accountability Office[5] or Congressional Research Service.[6]

Box 11.1 BLUF Example[7]

Competition among countries will increase in the coming year as major powers and regional aggressors exploit complex global trends while adjusting to new priorities in US foreign policy. The risk of interstate conflict, including among great powers, is higher than at any time since the end of the Cold War. The most immediate threats of regional interstate conflict in the next year come from North Korea and from Saudi-Iranian use of proxies in their rivalry. At the same time, the threat of state and non-state use of weapons of mass destruction will continue to grow….

> Tension within many countries will rise, and the threat from Sunni violent extremist groups will evolve as they recoup after battlefield losses in the Middle East….
>
> ODNI 2018 "Worldwide Threat Assessment"

Depending on the type of written report or verbal briefing, the BLUF may be supported in the same section by additional information. This is especially true in executive summaries. The purpose or question(s) for the analysis are usually part of the BLUF. Further, the BLUF should make clear if the report or briefing is in response to a specific customer request, part of other formal analytic tasking, or as the result of a current event or recent development. The BLUF also may be supported by important background or contextual information, especially when the background or context clarifies the linkage between the purpose of the report and contentions. Providing the basics of *who, what, where, when*, and *how* of the situation also may be appropriate in a longer BLUF. The most important factor to remember is that busy decision makers may only read the BLUF. Think of the BLUF in shorter written reports as the "30-second elevator talk," which conveys the purpose, main findings, and key information to the customer in the shortest time. A good BLUF should entice the reader or listener to want to learn more from the longer written report or verbal briefing.

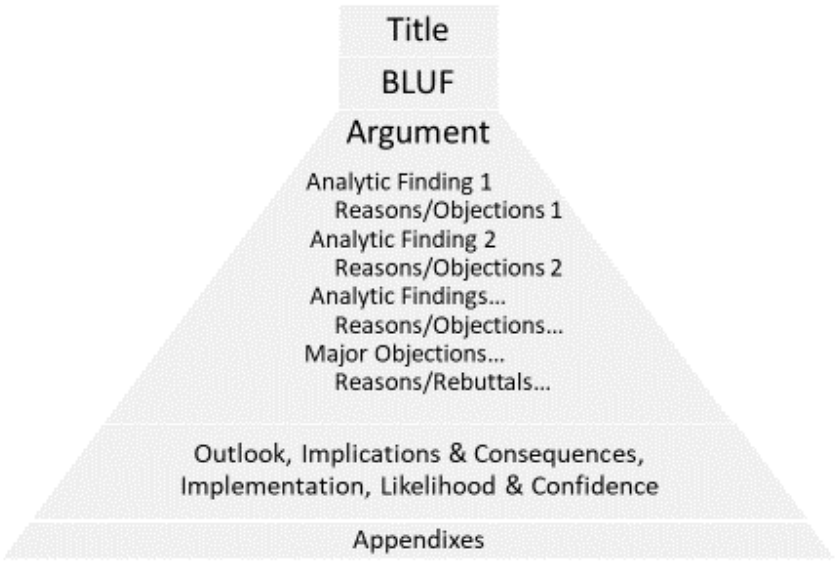
Building the Argument

A good **argument** makes up the main body of a report or briefing. As with other types of professional or academic documents, drafting a security analysis written report or verbal briefing should start with an outline. The objective of the outline is to "…create a roadmap for writing [the]…paper down to the paragraph level."[8] Security analysis written reports or verbal briefings employ a top-down "pyramid" approach as depicted in Figure 11.1.[9] This approach calls first for the title and

BLUF, which are followed by the argument or main body of the report providing detailed **reasons, evidence, and objections** that support the BLUF.

The argument supports the contentions of the analysis. This includes the evidence, reasons, and objections that also support each **analytic finding**. The first sentence of each new argument point should be an analytic finding. Each argument point could be one paragraph or a series of paragraphs, with all argument paragraphs starting with an analytic insight or finding. An argument is organized in priority order, with the most important analytic finding provided first, followed by the other analytic findings in descending order of importance. **Major** o**bjections** to the analytic findings and **rebuttals** to those objections also are important components of the argument section. This recommended format follows the logical argumentation outline presented in Chapter 9.

Figure 11.1 Outline For Security Analysis Presentation



Finishing Touches

After the title, BLUF, and argument of a written report or verbal briefing comes the **finishing touches**, which are items complementing or enhancing the

argument or main body of the report or briefing. In security analysis, these finishing touches should answer questions the reader or listener may have about the BLUF and arguments. Most written reports do not require a formal conclusion because the BLUF provided at the beginning summarizes the results of the analysis. There are some items; however, that may need to be provided later in a written report to support the BLUF and arguments. If the project's purpose or question(s) did not specifically call for a predictive (*what will happen?*) analysis, it may be helpful to include an **outlook** discussion that highlights what to expect next in the event or development. If a "*what next*" analysis was part of the BLUF and arguments, then an outlook is not required. Also, if not addressed in the BLUF or arguments, the **implications** and/or **consequences** of the analysis concerning the contentions about the event or development also may be included near the end of a written report or verbal briefing. See Chapter 10 for specifics on developing implications and consequences. In a security policy analysis report or briefing, there should be a summary of the initial implementation plan for the recommendations, including any anticipated resistance to the recommendations. See Chapter 10 for details.

One item that must be in all intelligence analysis reports and briefings, and also may be appropriate for security policy reports and briefings, is the analyst's determination of the **uncertainty** associated with the analytic results. This uncertainty usually is expressed in terms of **likelihood** and **confidence levels**. Likelihood focuses on the likely occurrence of the explanation for an event or development, likelihood of any predictions about the event or development, or likelihood of the report's recommendations to solve the problem addressed. Confidence levels capture the analyst's assessment of the quality of their overall analysis. In addition to the analyst's estimates of likelihood and confidence levels, the written report or verbal briefing must indicate the causes of the uncertainty (information, sources, assumptions, models, etc.). The differences between likelihood and confidence levels often confuse readers or listeners; to avoid this, the Office of the Director of National Intelligence (ODNI) cautions that analysts

"must not combine a confidence level and a degree of likelihood…in the same sentence."[10]

Likelihood, which refers to the analyzed actor's past or future behaviors in an event or development, may be expressed in statements, probabilities (either in words or numbers), or other likelihood measures such as odds (1 chance out of 5, 2 chances out of 3, etc.). The main factor in determining likelihood is the analyst's subjective estimate of how likely the event or development being explained or predicted did or will occur. Remember when analyzing human behavior, the world is probabilistic and not deterministic. This means while a human target may have acted one way in the past, or an event or development unfolded one way in the past, does not mean the same behaviors will be identical in the future; so, behavior tends to be very probabilistic. In order to standardize how likelihood and probability are expressed in intelligence reports and briefings, the ODNI provides the guidance summarized in Figure 11.2.

Figure 11.2 Expressing Likelihood and Probability[11]

almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain
remote	highly improbable	improbable (improbably)	roughly even odds	probable (probably)	highly probable	nearly certain
01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%

Confidence levels are the analyst's subjective assessment of the quality of their judgments. Analysts therefore must reflect on the quality of their information, sources, information gaps, assumptions, models, and analytic methods to determine their overall confidence in the report's findings. For confidence level assessments in quantitative studies, the analyst should consider the *statistical significance* (p-value) of the computational results. The statistical significance is expressed as numeric probabilities (0 (least) to 1.0 (most)). In the social sciences (including security analysis), a statistical significance of .05 is normally the standard, indicating the results would be accepted but could still be

wrong in 1 out of 20 cases. This also means the results are likely correct 19 out of 20 times or a 95% or high confidence level. Comparative analyses employ a *benchmark proportion* assessment—simply indicating the percentage of cases studied meeting the analytic findings. In qualitative analysis, there are no statistical or mathematical measures to assist in determining confidence levels, so the analyst must rely on a subjective estimate. The final confidence levels usually are stated as low, moderate, or high. Figure 11.3 provides the definitions of confidence levels used in the U.S. Department of Homeland Security.

Figure 11.3 Department of Homeland Security Confidence Levels[12]

High Confidence generally indicates that judgments are based on high-quality information from multiple sources or from a single, highly reliable source, and/or that the nature of the issue makes it possible to render a solid judgment.

Moderate Confidence generally means that the information is credibly sourced and plausible, but can be interpreted in various ways, or is not of sufficient quality or corroborated sufficiently to warrant a higher level of confidence.

Low Confidence generally mean that the information's credibility and/or plausibility is questionable, the information is too fragmented or poorly corroborated to make solid analytic inferences, or there are significant concerns or problems with the sources.

Finally, security analysis written reports usually provide one or more supporting **appendixes**. The appendixes may include a number of different types of information to include historical or background material, organizational information on actors in the analysis, details on information sources, worksheets or results of the analytic methodology, technical or scientific information, or any additional supporting or peripheral information the reader may reference to better understand the report.[13] Information is placed in appendixes to not overburden the BLUF or argument sections of the report. Chronologies of the

event or development under study are commonly provided in appendixes. Annotated charts or maps also are common in appendixes, with annotations limited to those assisting the reader's understanding of the analysis. Detailed statistical data presented in tables and graphs also is common in appendixes. If needed to support questions about the report or briefing; or, if needed for the review process (presented later), the analyst may include worksheets employed in the analysis. Worksheets can include Quality of Information Checks, Four Ways of Seeing + Analyst, Assumptions and Beliefs analysis, conceptual model diagrams, or other details of the analytic methods used in the analysis. In an intelligence threat analysis report, appendixes should be included for creating an Intelligence and Warning (I&W) Problem, including an Indicators Analysis and its supporting intelligence collection plan. In a security policy analysis report, a detailed implementation plan is appropriate in one or more appendixes. Verbal briefings do not have appendixes, but the analyst may have additional slides available as supporting material in case they are needed to assist in the question-and-answer period. It is the analyst's prerogative as to what goes into the appendixes, provided the information supports and helps clarify the written report or verbal briefing's BLUF and arguments.

Guidance for Preparing Written Reports

Written reports must be precise, clear, accurate, consistent, digestible, and of a complexity level that does not confuse the reader. The following general guidance provides guidance on preparing written reports.

Answer the questions. Often a security analysis project will wander off-track and fail to answer the questions asked at the start of the project. Make sure the report is consistent from the title and BLUF through the final appendix. The report focus must remain on the original purpose and questions. The overall report must anticipate and answer the questions customers or audiences may

have about the analysis. Thus, ensure the 5Ws + 1H questions (see Figure 8.1) are answered clearly. Additionally, make sure there is a focus on the "*what, why now, impact so far, what next,* and *implications,*" as appropriate, for the analysis at hand. These are the pillars of what the written report must convey to customers and audiences.[14]

Build strong paragraphs. Every paragraph in the argument should start with a topic sentence that contains an analytic insight or finding. Only one analytic insight or finding should be addressed per paragraph. A second strong sentence should provide context for the analytic insight or finding, elaborate on the topic sentence, and bridge the topic sentence to the rest of the paragraph.[15] The remaining sentences present evidence (information, data, facts) and reasons (logic) that support the analytic insight or finding. Ensure there are logical and easily understandable linkages between evidence and reasons that offer a smooth and consistent flow of information. Some of the words used to link evidence and reasons to build a good argument include:[16]

as	follows from	in view of the fact that
as indicated by	for	may be deduced
as shown by	from	may be derived from
assuming (that)	given (that)	may be inferred from
because	in as much as	since
due to	in so far as	the reason is that

Words to introduce findings or conclusions based on evidence and reasons include:[17]

accordingly	*ergo*	implies that
as a result	for these reasons	in consequence
conclude that	for this reason	is evidence that

is reason to believe	therefore	which implies that
is reason to hold	thus	which means that
it follows that	we may infer	which points to
hence	which allows us to	
means that	infer	
so	which entails that	

Display important evidence. Security analysis relies on qualitative or quantitative evidence~~,~~ or a combination of both. Similar to the Chapter 9 guidance on pattern-matching analyses, evidence may be presented in many ways:[18]

- Direct quotations from conversations, speeches, interviews, existing reports, articles, books, etc.
- Observations by intelligence collectors, diplomats, media personnel, etc.
- Words representing objects, images, or events using anecdotes, narratives, or descriptions.
- Ground-truth photographs, overhead imagery, charts, maps, videos, voice recordings, communication intercepts, etc., representing objects or events visually or aurally.
- Figures, tables, diagrams, graphs, boxes, charts, or maps.
- Summaries and paraphrases of any of the above.

Use graphics widely. The old adage of "a picture is worth a thousand words" applies directly to security analysis reports. Graphics—especially figures, tables, diagrams, charts, maps, etc.—may be included to support the report's arguments or the finishing touches discussed previously. Avoid placing large graphics in the main body of the report, as it is usually best to place them in an appendix if they run more than a half to three-quarters of a page. Where the

graphic is placed or first mentioned in the report text, a narrative description of the graphic contents must be provided so the reader better understands the information. Remember; however, that graphics alone do not tell the story, but good graphics can be valuable additions.

Do not describe the analytic process. Written reports present and support the analytic findings of the security analysis project. Keep in mind; however, that customers do not want a detailed description of how the findings were generated or presented. Nor do they want to read the words "bottom-line-up-front" or the acronym "BLUF" in the text of any report. Focus instead on presenting the insights and findings that resulted from the critical-thinking analysis. If customers want more details on how the analytic findings were generated, they will ask. There are a couple of exceptions to this guidance. First, sometimes an analytic figure, graphic, table, etc., used in reaching the findings may help the audience understand the report. As mentioned earlier, if one large figure, graph, or table extends to more than half to three-quarters of a page, it should be placed in an appendix; if smaller, it may be a candidate for placement in the report's main body. For example, when using a matrix analysis method, such as an Analysis of Competing Hypotheses, placing that matrix in the main body or in an appendix may help the customer better understand the findings. Second, if the report goes through a formal review process before publication, either by supervisors or through a Devil's Advocacy challenge process (detailed later), then it is appropriate to place the worksheets from the analytic process in appendixes or in a separate folder for reviewer reference.

Avoid logic fallacies. Use of **logic fallacies** can result in defective arguments that degrade the validity of the report's analytic findings. A logic fallacy makes claims in reasoning or evidence that do not support a valid finding or conclusion. Formal logical fallacies usually are easy to detect as they result from untruthful information, obviously bad assumptions, or major flaws in reasoning. Informal

logic fallacies often are more difficult to detect, but they are used widely in societal discourse and are easily overlooked because they are so frequently used, even by analysts. Appendix I provides a summary of frequently encountered informal logic fallacies seen in security analysis. Analysts must ensure the linkage of evidence and reasoning that leads to analytic findings does not commit one or more formal or informal logic fallacies. The presence of logic fallacies reduces the validity of the analytic findings and the veracity of the overall contentions of the analysis.

Use proper English. Analysts must follow the grammar, spelling, punctuation, and abbreviation guidance in their home organization's style guide. Word processor spelling and grammar checkers are highly recommended. Some common English and structural writing mistakes to avoid in professional reports include:

Use active voice. Security analysis written reports are written in the active voice, which is when the subject of the sentence performs the action of the sentence verb. Active voice sentences indicate the subject and verb, and then demonstrate the action is being performed by the subject. In passive voice, the subject is usually the receiver of the action. Examples:

> Passive Voice (avoid): The World Trade Center was attacked by the terrorists.
> Active Voice (best): Terrorists attacked the World Trade Center.

Some word processors calculate the percentage of active and passive voice in a document. Not all passive voice must be avoided as the readability of the report may improve with an occasional sentence in passive voice; but, make sure the main narrative of a report is primarily in the active voice.

Write in third person. Minimize or avoid any use of first person (I, me, we, etc.) and second person (you, your) in security analysis reports and briefings (except in quotes from other parties). Many reports and briefings will be published to larger audiences where the first person or second person makes little sense.

Eliminate contractions. It is not appropriate to use contractions in formal writing. Spell out the words rather than employ common contractions.

Avoid expressing opinions. Do not include wording such as "In my opinion….," "I think….," I believe….," I feel….," or other similar phrases. Not only are such statements not in third person, but customers do not want to hear opinions or feelings. Instead, they want analytic findings based on solid evidence and reasoning resulting from an active and systematic analysis. Remember: "Provide Good Analysis Not Opinions!"

Avoid rhetorical or hypothetical questions. Rhetorical questions are used to emphasize a point in a narrative and are not expected to be answered. For example: "Why would anyone want to study security analysis?" Hypothetical questions usually point to important evidence or causality in an argument; but, in effect, the evidence and or causality is wrong and has no effect on the issue under study. For example: "Is it not clear Country Z started the war to improve its economy?" (With no evidence to support the claim, it is probably not clear.) The only questions in a security analysis should be those resulting from the purpose and question elements in the critical-thinking process. Save the rhetorical and hypothetical questions for short stories and novels.

Avoid colloquial sayings. Colloquial sayings are words, phrases, or sayings used in informal communications, but are not appropriate in professional

or academic reports or briefings. Analysts should not write the way they speak. For example, never write words such as "this study does not *hold water*." Instead write "this study has problems with its evidence and reasoning."

Avoid value-laden statements. These types of statement offer the analyst's subjective and often-biased perception of a situation, which could be either good or bad. For example, avoid wording such as "the United States is the most powerful nation on Earth, therefore…." Customers do not want to see or hear such exaggerations supporting an argument.

Provide a readable text. Make sufficient use of main headings and sub-headings throughout the report to break up the text and provide the reader a logical outline of the report. The home organization's style guide usually will provide the formatting for headings. Readers prefer a layout that includes white space. Pages should include at least two or three paragraph starts, and each paragraph should normally contain at least three sentences.

Document everything. Make wide use of either bibliographic in-text citations, endnotes, footnotes, or other procedures for documenting the sources of the analysis as called for in the home organization's style guide or by other supervisory guidance. In academic circles, not thoroughly documenting sources is plagiarism. In practitioner circles, not documenting sources is unprofessional, usually unethical; and in commercial circles, might result in a lawsuit.

Proofread, proofread, proofread. Even when the written report is a draft be sure to proofread and continue proofreading before and throughout the self-review, structured self-critique, and Devil's Advocacy challenge process discussed

below. Make maximum use of word processor spelling and grammar checkers. Be careful as some words will pass a spell check because they are spelled correctly, but will not be correct for the context of the report. For example, the words "border" and "boarder" will both pass a spell check, but mean far different things. Once an analyst has worked on a written report in a digital file format for a long time, they may overlook simple errors because they have seen and not corrected those errors numerous times. It is useful to have a colleague not involved in the project to proofread the report. Always print and proofread a written copy of the report to uncover any errors not readily found in an on-screen digital file format. Also, make at least one proofreading review where only the topic sentences of each paragraph are read; this helps ensure the analytic findings are understandable and consistent.[19]

Guidance for Verbal Briefings

Verbal briefings offer some unique challenges. In general, all the guidance above for written reports also applies to verbal briefings. The following is additional guidance on preparing verbal briefings:

Murphy will be there. Murphy's Law states "Whatever could go wrong, will go wrong." This applies a hundred times over to verbal briefings. For example, most briefings consist of digital slides produced with MS PowerPoint or other presentation software. If planning a digitally supported briefing, the analyst should have a back-up plan if the computer or projector fails (e.g., ensure spare equipment or spare bulbs are available), the digital file is corrupted (have paper copies), or other electronic problems are encountered. It is always a good idea to have paper back-ups for the main customer(s) when planning digital-supported briefings. Paper copies also can be handed out after the briefing. If the briefing is scheduled for 20 minutes and the customer arrives 10 minutes late, have a plan

to reduce the briefing to 10 minutes. It is best to have a back-up plan for any problems that may occur.

Give the customer a break. It is possible that the customer and audience for a verbal briefing may not have read the corresponding written report. It is important; therefore, to construct a verbal briefing that is informative and persuasive and does not lose the customer and audience. There is an adage that the best briefings will "tell them what you are going to tell them (the BLUF), then tell them (the argument), and then tell them what you told them (the BLUF again)." This is good advice for most verbal briefings, especially because after five to seven minutes, the attention of listeners may start to wane. Do not use slides that contain dense narratives. Use a "bullet" (short statement) format for key findings, evidence, and reasoning; the presenter can then fill in the details with their actual briefing. Use of photographs and graphics are strongly recommended, but select such material only if it directly supports evidence and reasoning in the briefing. Keep graphics professional; i.e., do not use more than three colors, avoid moving characters, and eliminate complex graphics. Make sure digital briefing slides are readable in the back of the room. Spend no more than three-quarters of the time allotted delivering the verbal briefing so there is time for a question-and-answer (Q&A) period. It is best not to go over the allotted time for the briefing. Time may be exceeded to extend the Q&A period provided the customer and audience agree. Remember: The goal is to inform and persuade the customer and audience and to do so in a clear, precise, and accurate manner.

Practice. practice, practice. Do not assume the verbal briefing will fill the time available. Practice the briefing and time the sessions to make sure it can be completed in the allotted time. Most busy customers do not appreciate briefings running over. Video record the initial practice sessions and also have colleagues listen to live verbal briefing practices and request they make comments on how it may be improved. When colleagues and immediate supervisors provide critical

feedback on a briefing, it often is referred to in government and military circles as a “murder board.” Remember the 5 P’s: Prior Planning Prevents Poor Performance!

Reviewing the Report or Briefing

Review and critique of a written report or verbal briefing is critical to its quality and effectiveness. In the active and systematic process of critical thinking, there are a number of checks on the quality of the actual analysis; they include assessing the quality of information, investigating potential deception, assessing points of view and assumptions, generating conceptual models, using analytic methods to reach findings, and generating implications and consequences of the findings. However, the initial draft of written reports and verbal briefings still requires the analyst (or analytic team) and supervisors to conduct a robust review and critique. Feedback from colleagues and supervisors is important.

In this book, a three-part review and critique process is recommended. First, complete a deep, structured self-critique focusing on the veracity of the analytic findings. Second, the drafts of written reports and verbal briefings undergo a critical self-review. Third, intelligence-related written reports may be submitted to a **challenge analysis Devil’s Advocacy** process. A Devil’s Advocacy challenge analysis seeks to refute the report’s findings through a review of the analytic process and by attempting to use the same evidence to reach different findings.[20] Such a process also is recommended for security policy analysis reports. After the Devil’s Advocacy process is complete, the written report can be published. This process mainly applies to strategic or operational reports without sensitive time limits for report submission. Time-sensitive, current event or tactical reports and briefings likely will only undergo the analyst’s (or analytic team’s) structured self-critique, self-review, and a supervisory review before publishing.

Start the review with an assessment of the draft report or briefing's analytic findings through a **structured self-critique**. This is a deep review of the analytic process used to reach the findings, because it is better to identify why the findings are wrong before the report is published or briefing given than to have to later explain why it was wrong.[21] It may take only a couple of hours to conduct a structured self-critique and identify problems early, or it could take days or weeks to later explain to angry customers why the analysis was wrong.

In a structured self-critique, the analyst goes back through the entire analysis and examines the analytic process to see what factors might lead to the analytic findings being wrong. Figure 11.4 provides a list of the key questions analysts must consider to help avoid errors.[22] As a result of the structured self-critique, the analyst may need to revisit each of the critical-thinking elements used to reach the analytic findings and make revisions to the latest draft.

Figure 11.4 Structured Self-Critique Key Questions[23]

What if my main conclusion or key judgment turns out to be wrong?

- How reliable was the key evidence?
- Were there significant information gaps?
- What should the absence of information indicate?
- Was contradictory evidence ignored? If so, why?
- Was past or emerging contexts ignored?
- Did deception go undetected?
- Were assumptions and beliefs critically evaluated and deemed valid?
- Was a broad range of diverse perspectives solicited?
- Were alternative explanations or hypotheses considered?
- Were both agency and structural factors considered?
- Was a critical-thinking framework followed?
- Were common analytic pitfalls avoided?

The latest draft of the written report or verbal briefing should then undergo a **self-review** of its critical-thinking **Intellectual Standards,**[24] detailed in

Figure 11.5. The Intellectual Standards check on the quality of the critical thinking used in the analysis and the quality of the draft written report or verbal briefing. Both the entire draft and each major analytic finding should be examined through the Intellectual Standards checklist. Depending on the type of report or briefing, other standards the analyst may consider include whether the critical thinking and draft report or briefing are *reasonable, consistent, falsifiable, testable, well organized, authenticated, effective,* and/or *factual*.[25] As a result of the self-review, the analyst may find a need to revisit the elements of thought used to reach the analytic findings and make revisions to the draft.

Figure 11.5 Checklist for Intellectual Standards Assessing Critical Thinking[26]

_____Clarity

Could you elaborate?

Could you illustrate what you mean?

Could you give me an example?

_____Accuracy

How could we check on that?

How could we find out if that is true?

How could we verify or test that?

_____Precision

Could you be more specific?

Could you give me more details?

Could you be more exact?

_____Relevance

How does that relate to the problem?

How does that relate to the question?

How does that help us with the issue?

_____Depth

What factors make this difficult?

What are some of the complexities of this question?

What are some of the difficulties we need to deal with?

_____**Breadth**

Do we need to look at this from another perspective?

Do we need to consider another point of view?

Do we need to look at this in other ways?

_____**Logic**

Does all of this make sense together?

Does your first paragraph fit in with your last one?

Does what you say follow from the evidence?

_____**Significance**

Is this the most important problem to consider?

Is this the central idea to focus on?

Which of these facts are most important?

_____**Fairness**

Is my thinking justifiable in context?

Am I taking into account the thinking of others?

Is my purpose fair given the situation?

Are concepts clear?

Am I distorting concepts to get what I want?

Once the self-review using the Intellectual Standards is completed and appropriate revisions made, the analyst should feel confident in placing the revised draft of written reports into the challenge analysis process. At this point, the analyst can provide the draft to their supervisors and/or the home organization's **Devil's Advocacy** process. This structure may be a comprehensive supervisory review or a more formal Devil's Advocacy process managed by a separate office or staff. Verbal briefings usually are reviewed only by supervisors and do not normally undergo challenge analysis. In the IC, challenge analyses seek

to refute the report's findings through a review of the analytic process and by attempting to use the same evidence to reach different findings. It also includes the analytic standards published by ODNI in Intelligence Community Directive (ICD) 203,[27] which also pertains to security policy analysis reports and should be used as appropriate. Figure 11.6 summarizes the ICD 203 requirements.

Upon completion of the structured self-critique, self-review with the Intellectual Standards, and the Devil's Advocacy challenge process, a written report should be ready for publication. Verbal briefings also will be ready for delivery upon completing any "murder boards" and supervisory reviews. This is the culmination of a security analysis project. The analyst will have taken their project from the critical-thinking purpose and question elements through each critical-thinking element leading to the final written report and/or verbal briefing. The critical-thinking elements require a more robust process of thinking and analysis than what most new analysts or academic students have experienced in the past. The more the analyst uses this analytic process, the more proficient they will become.

Figure 11.6 Checklist for ICD 203 Analytic Standards[28]

_____Analysts must perform their work with objectivity and with awareness of their own assumptions and reasoning.

_____Analytic assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint.

_____Analysis should be informed by *all* relevant information available.

_____Analysis must exhibit analytic tradecraft standards, specifically:

_____Properly describe quality and credibility of underlying sources, data, and methodologies.

_____Properly express and explain uncertainties associate with major analytic findings.

_____Properly distinguish between underlying information and analysts' assumptions and judgments.

_____Incorporate analysis of alternatives.

_____Demonstrate customer relevance and addresses implications and consequences.

_____Use clear and logical argumentation.

_____Explain change to or consistency with past analytic judgments.

_____Makes accurate judgments and assessments.

_____Incorporates effective visual information where appropriate.

_____Analysis must be disseminated in a timely manner to be actionable by customers.

Key Concepts

Analytic Findings
Appendixes
Argument
Argument Map
BLUF
Challenge Analysis
Confidence Levels
Consequences
Contention
Devil's Advocacy
Evidence
Executive Summary
Finishing Touches
Implications
Intellectual Standards
Likelihood
Logic Fallacies
Objections
Outlook
Rebuttals
Reasons
Structured Self-Critique

Title **Verbal Briefings**

Uncertainty **Written Reports**

Discussion Points

1. Why are the general humanities and scientific method writing approaches not appropriate for writing security analysis intelligence or policy reports?
2. Why is the bottom-line-up-front (BLUF) approach used for security analysis written reports and verbal briefings?
3. Why must argument objections and rebuttals be included in security analysis written reports and verbal briefings?
4. Select your last analytic paper and compare it to the material in this chapter. What did you do right and what did you do wrong in preparing this paper?
5. Compare and contrast the review process you used in the past to the techniques covered in this chapter for structured self-critique, self-review, and Devil's Advocacy. How will you review your reports and briefings in the future?

Notes

[1] Louis M. Kaiser and Randolph H. Pherson, *Analytic Writing Guide* (Reston, VA: Pherson Associates, LLC, 2014), 21.

[2] Katherine Hibbs Pherson and Randolph H. Pherson, *Critical Thinking for Strategic Intelligence*, 2nd ed. (Thousand Oaks, CA: SAGE/CQ Press, 2017), 248-249.

[3] Ibid, 251.

[4] Eugene Bardach and Eric M. Patashnik, *A Practical Guide for Policy Analysis, The Eightfold Path to More Effective Problem Solving*, 5th ed. (Thousand Oaks, CA: SAGE/CQ Press, 2016), 78.

[5] U.S. Government Accountability Office, "Reports and Testimonies," https://www.gao.gov/browse/topic (accessed August 3, 2018).

[6] Library of Congress, Congressional Research Service, "Areas of Research," https://www.loc.gov/crsinfo/research/ (accessed August 3, 2018).

[7] Daniel R. Coats, "Worldwide Threat Assessment of the U.S. Intelligence Community (Washington DC: Office of the Director of National Intelligence, 2018), https://www.dni.gov/files/documents/Newsroom/Testimonies/2018-ATA---Unclassified-SSCI.pdf (accessed July 23, 2018).

[8] Kaiser and Pherson, 22.

[9] Modified from Kaiser and Pherson, 23.

[10] Office of the Director of National Intelligence, "Intelligence Community Directive 203 Analytic Standards," (Washington, DC: Office of the Director of National Intelligence, 2015), 3 https://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf (accessed July 20, 2018).

[11] Ibid.

[12] Reprinted with U.S. government permission in Pherson and Pherson, 220.

[13] Kaiser and Pherson, 57-58

[14] Ibid, 13-20.

[15] Ibid, 39.

[16] Noel Hendrickson et al., *The Rowman and Littlefield Handbook for Critical Thinking* (Lanham, MD: Rowman and Littlefield Publishers, Inc., 2008), 13.

[17] Ibid, 13-14.

[18] Wayne C. Booth, Gregory G, Colomb, and Joseph M. Williams, *The Craft of Research*, 2nd ed. (Chicago, IL: The University of Chicago Press, 2003), 144-145.

[19] Kaiser and Pherson, 71.

[20] See discussion in Morgan D. Jones, *The Thinker's Toolkit, 14 Powerful Techniques for Problem Solving*, rev. ed. (New York, NY: Three Rivers Press, 1998), 217-220. Detailed procedures for several challenge analysis techniques are found in Richard J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence Analysis*, 2nd ed. (Thousand Oaks, CA: SAGE/CQ Press, 2015), 233-272.

[21] Pherson and Pherson, 196-199.

[22] Figure modified from Pherson and Pherson, 198-199. The structured self-critique technique is defined in more detail in Heuer and Pherson, 245-249.

[23] Ibid.

[24] Richard Paul and Linda Elder, *Critical Thinking, Tools for Taking Charge of Your Professional and Personal Life*, 2nd ed. (Upper Saddle River, NJ: Pearson Education, Inc., 2014), 127-166.

[25] Gerald M. Nosich, *Learning to Think Things Through, A Guide to Critical Thinking Across the Curriculum,* 4th ed. (Upper Saddle River, NJ: Pearson/Prentice Hall, 2011).

[26] Paul and Elder, 141-142.

[27] Office of the Director of National Intelligence, 2-5.

[28] Ibid.