Date:	12-Apr-23	Document Number:	230412-article-yardstick-frank-cap10
Revision:	1	Author:	Frank Cannon CSyP, FSyI

PROFESSIONAL HEAD OF INTELLIGENCE ASSESSMENT PROBABILITY YARDSTICK

A Curious Question Promptly Answered by The Security Institute

1. Introduction

1.1. At five o'clock on the afternoon of 10th April 2023, I posed a question on *The Security Institutes*[1] (The SyI) Member's Area Community chat forum. Within ten hours, I received multiple responses, a very comprehensive explanation of my query, and various links to further reading.

1.2. This is the true benefit of professional membership associations — and specifically The SyI. Demonstrating therefore, that learning from your peers and professional colleagues helps satisfies a curious mindset that I believe is required by all those that protect others.

2. The Question

2.1. Is anyone else curious as to the design of the 'probability yardstick' that the Cabinet Office issued to standardise HM Government's intelligence assessments? Why is it so complex and, for me at least, seems illogical.

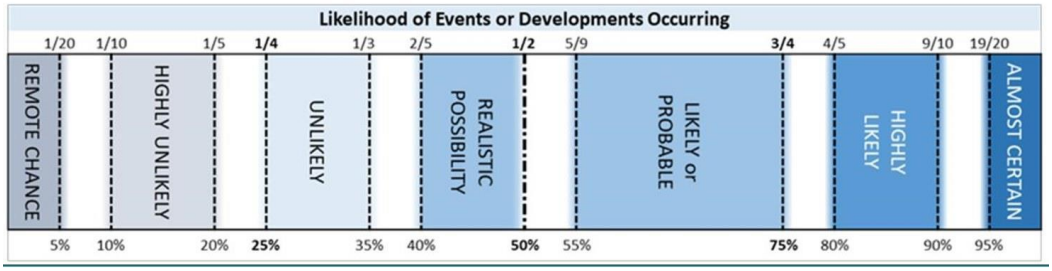


Figure 1: Probability Yardstick

2.2. Firstly, there are seven (7) levels of likelihood that an event might occur – most of us would use a standard 5 x 5 risk matrix, and when determining the likelihood, I typically draw information from a preceding threat assessment. Therefore, when categorising the likelihood of a terrorist attack occurring, one would then carry this 'score' across to the likelihood axis within the adversarial risk matrix. Would I not?

2.3. Secondly, why is there a need to use the fractional scale along the top of the yardstick, i.e., 1/20 or 4/5, or 19/20? Or am I reading this wrong? I do understand the inclusion of the percentage scale along the bottom as most people would say, "*there's a 30% probability that…"*

2.4. Finally, why are there gaps between the seven named elements of the yardstick? What if the probability was 8%, 37%, or 76%. Why doesn't each of the seven named elements butt up against one another so there is a continuum of threat scoring?

2.5. I've read the guidance on the NPSA website [last updated on 10 Feb 22] but it doesn't explain the logic behind this government probability yardstick.

[1] The Security Institute is a professional body which was established in 1999 to promote a clear understanding of security and professionalism in the business of security. Central to this vision is the objective of raising the profile of the security profession and those who practice in it, in the eyes of those who come into contact with it.

Location: South Mill Road, Amesbury, SP47HR. UK I. Mobile: +44 (0)7742 569943 I Email: frank@cannonassetprotection.uk I Website: https://thecapway.com/

2.6. Does anyone know who the author was, what their logic is, and does anyone else use it other than those in government departments? Does anyone else care!

3. Executive Summary (bottom line up front[2])

3.1. I now recognised that there is a logic to this measurement tool. It is not too complicated and provides the necessary nuance when communicating uncertainty.

3.2. I discovered that the agreed standard for conveying probability in intelligence analysis in the UK is the 'PHIA Probability Yardstick'. This is a scale of probabilistic language developed by Defence Intelligence and latterly adopted by the Professional Head of Intelligence Assessments (PHIA) for use across the government intelligence community. The scale comprises accepted intelligence terminology at a national level.

3.3. Sir David Omand explained that the gaps in the PHIA Probability Yardstick avoid the potential problems that can be found in those scales without gaps. He highlighted the difficulty when deciding what term, you use if your judgement is *'around 20 per cent'*. Two analysts can have a perfectly reasonable argument over whether something is 'very unlikely' or 'unlikely'. He argues that the gaps in the Yardstick obviate the problem.

3.4. I discovered that SyI professionals do care! However, I didn't receive an explanation for the fraction range along the top of the Yardstick[3] other than to cater for those who prefer expressing probability as a fraction rather than a percentage.

4. The Responses

4.1. ***Hot Topic*** – posted by Bruce B:

4.1.1. This is probably the most controversial and hotly debated subject in security risk assessment. You bring up some interesting questions, however at the end of the day after over 45 years in this game, I reckon the answer is: '*Do what works for you and your organisation'*. Honestly, I am now adopting an approach that simplifies the "*measurement*" in assessments rather than trying to produce quantified assessment as I don't believe security risk can be "*quantified*" due to the dynamic nature and the human drivers.

4.2. ***Poor Understanding*** – posted by Ken W:

4.2.1. I agree with Bruce that this is a really important topic which is poorly understood. I used a masters to explore this subject a few years ago. In essence, it is very difficult to try to shoe-horn very high impact-low occurrence events into this type of numerical system.

4.2.2. Where data is small, as in numbers of incidents, it leads to a high degree of uncertainty in the "level" given to that future event probability. This uncertainty is rarely then described correctly. Some would call it pseudo-science.

4.3. ***Why the Gaps*** – posted by Harry S:

4.3.1. Writing in 'How Spies Think - Ten Lessons in Intelligence', Sir David Omand, former Cabinet Office Intelligence and Security Coordinator and former Director of GCHQ, explains the gaps as

[2] Read on if you want to know where BLUF comes from.

[3] The use of the vernacular 'Yardstick' is an accepted term meaning 'a measure or standard use of comparison'.

"...to avoid the potential problem with the United States scale (with no gaps) over what term you use if your judgement is 'around 20 per cent'. Two analysts can have a perfectly reasonable, but unnecessary, argument over whether something is 'very unlikely' or 'unlikely'. The gaps obviate the problem. The challenge is over what to do if the judgement falls within one of the gaps. If an analyst can legitimately say that something is 'a 75-80 per cent chance', then they are free to do so. The yardstick is a guide and a minimum standard, but analysts are free to be more specific or precise in their judgements, if they can. It is sensible to think in 5 or 10 per cent increments to discourage unjustified precision for which the evidence is unlikely to be available. I recommend this framework in any situation in which you have to make a prediction. It is very flexible, universally applicable, and extremely helpful in aiding your decision making and in communicating it to others. You could start off by reminding yourself the next time you say it is 'unlikely' to rain that that still leaves a one in five chance of a downpour. You might well accept that level of risk and not bother with a coat. But if you were badly run down after a bout of flu even a 20 per cent chance of getting soaked and developing a fever would be a risk not worth running. That is an example of examining the expected value of the outcome, not just its likelihood, formed by multiplying together the probability of an event and a measure of the consequences for you of it happening."

4.4. ***Links to the NIM*** – posted by Lee C

4.4.1. As I understand it this is in alignment with the National Intelligence Model so that there is consistency in approach and common language regarding assessments, including probability.

4.4.2. You will find a lot more detail on the College of Policing website:

https://www.college.police.uk/app/intelligence-management/analysis/delivering-effective-analysis

4.5. ***Quick Wins for Busy Analysts*** – posted by Andy D *(Co-Chair of the CT Special Interest Group in the SyI Community Chat forum)*:

4.5.1. The link below is to the PHIA (Professional Head of Intelligence Analysis) 'Quick Wins for Busy Analysts' - page 53+ deals with 'communicating uncertainty' and 'the yardstick'. Whilst it's been a few years since I did the GIAT, the handbook is still a decent reference guide and may illuminate some of the fair issues you raise!

https://assets.college.police.uk/s3fs-public/2021-07/foia-2021-058.pdf

4.5.2. Annex A to this paper contains the extract from the freedom of information answer (FOIA) highlighted by Andy above.

4.6. ***MoRiLE and Beyond*** – posted by Chris D

4.6.1. I care!

4.6.2. During my time in Policing, I created and then led the Management of Risk in Law Enforcement (MoRiLE) Programme of work, that created risk models for Law Enforcement and our Partners. We used the Probability Yardstick within each of our models as it was a tool that was recognised across Law Enforcement and our Partners. We did not change anything within it but did simplify how it was seen by the end user as we utilised dashboards and drop-down menus for the MoRiLE models and called it a "Confidence Assessment" as we were assessing things that had happened, not probabilities. The use of the Yardstick was well received and worked well in terms of "nudging" people to use the yardstick language within their assessments, which further supported out aim of developing consistency. I have added a couple of links below that may be useful. (I am under the

same impression as the Protect website that this came from the PHIA and was then adopted by the cabinet Office)

4.6.3. The work we did within the MoRiLE Programme was trying to develop risk models that were more interactive, easier for end users, and richer in terms of the breadth of areas we could assess through one process. Again, this worked well, and the models were adopted extensively across Law Enforcement and Partners (used by all Police Forces and Law Enforcement agencies).

4.6.4. Probability Yardstick development: Post retirement I have developed a web-based risk solution (AURa) that is attempting to bring risk management to the masses and create a new discourse for risk management. We are trying to do this through the creation of system that is easy for the end users and helps them bring their organisational and operational risks management together in a way that looks and feels relevant to their daily business. We are taking this approach as we think there needs to be a new narrative and approach if we want people to add the management and documenting of risks into their already busy lives. This will be particularly relevant for small organisations that will be affected by the Protect Duty legislation, which is why we are creating a bespoke AURa Protect app that will bring together our models with the requirements of the legislation to help them create safe spaces and places.

4.6.5. Through the AURa app development work, I will be working on the creation of a range of scored considerations that sit underneath the probability yardstick that uses a range of factors that I believe over time can be automated. If this can be achieved, then we can explain the probability in a much richer way within the narratives of our assessments. The elements I plan to add are:

- Task Complexity
- Time Pressure
- Level of Expertise: Person(s) conducting the assessment
- Amount of Collaboration
- Use of Structured Methods
- Overall Source Reliability
- Source Congruency

4.6.6. History (Protect website) https://www.protectuk.police.uk/threat-risk/threat-analysis/complex-attacks

The Probabilistic Yardstick is a tool created by the Professional Head of Intelligence Analysis (PHIA), in the UK government, to standardise the way in which we describe probability in intelligence assessments.

Chris then posted a verbatim extract from the College of Policing website which I subsequently downloaded and included at Annex B to this paper.

4.7. ***NPSA Guidance*** – posted by Noel E

4.7.1. This may help to explain... A Guide to Using Threat Assessments | NPSA

Location: South Mill Road, Amesbury, SP47HR. UK I. Mobile: +44 (0)7742 569943 I Email: frank@cannonassetprotection.uk I Website: https://thecapway.com/

5. CONCLUSION - *Was it Worth Asking the Question?*

5.1. **Yes**! I have further developed my professional knowledge through tapping into the rich experience within my peer group. **So What**? I will integrate this new learning into an adversarial risk assessment tool that I have created as part of ***The CAP Way***. Every day is a learning day. I hope this paper helps others learn what I now know. ***The CAP Way*** website can be found here: https://thecapway.com/

5.2. Joining The Security Institute can provide numerous benefits to security practitioners, including access to cutting-edge security knowledge and skills, networking opportunities, and professional recognition. Through The Security Institute, members have access to a diverse range of CPD resources, such as training programs, webinars, publications, and events that can help them stay updated with the latest security trends and best practices.

5.3. Continuing professional development helps security professionals maintain their skills and knowledge, enhances their career prospects, and demonstrates commitment to their profession. CPD can also help security practitioners remain compliant with relevant industry standards and regulations, which ultimately increases their credibility and reputation in the industry.

5.4. By joining The Security Institute and engaging in CPD activities, security practitioners can also demonstrate their commitment to ethical behaviour and uphold high professional standards, which can enhance public trust and confidence in the security profession.

Apply to Join The Security Institute Here: https://security-institute.org/apply/

THE SECURITY INSTITUTE
FELLOW

Annexes:

A: FOI Request to the College of Policing.
B: Delivering Effective Analysis – College of Policing.

ANNEX A: FOI REQUEST TO THE COLLEGE OF POLICING

published on 16 Jun 21 (FOIA-2021-058) by Kate Kaufman | Legal Advisor. Information Management and Legal Team. College of Policing. Email: FOI@college.pnn.police.uk. Website: www.college.police.uk

COMMUNICATING UNCERTAINTY

"I told him that my personal estimate was on the dark side, namely that the odds were around 65 to 35 in favour of an attack. He was somewhat jolt-ed by this; he and his colleagues had read "serious possibility" to mean odds very considerably lower. Understandably troubled by this want of communication, I began asking my own colleagues on the Board of National Estimates what odds they had had in mind when they agreed to that wording. It was another jolt to find that each Board member had had somewhat different odds in mind and the low man was thinking of about 20 to 80, the high of 80 to 20. The rest ranged in between". Words of Estimative Probability (Sherman Kent, 1964).

INTRODUCTION

A1. The accurate communication of uncertainty is one of the most important elements of good intelligence assessment. When considering a course of action, policymakers must set its likely benefits against its likely costs: If they do not have a clear idea of the probability of various outcomes, the wrong decision might be made. Below are issues you should consider and guidance you should use when expressing probability and uncertainty.

THE PROBLEM OF COMMUNICATING UNCERTAINTY

A2. There are two key challenges to the analyst when communicating uncertainty: misinterpretation and misrepresentation.

Misinterpretation

A3. A significant challenge to communicating uncertainty is the risk of misinterpretation as there are no widely understood common definitions of probabilistic terms. One study showed that among a group of NATO military officers – with experience of reading intelligence reports – interpretations of the word 'probable' varied from 25% to 90% in terms of their understanding of the likelihood of an event taking place. This kind of finding, which has been replicated on a number of occasions, exposes a serious risk of misunderstanding by readers of intelligence assessments.

Misrepresentation

A4. In the absence of a common definition, readers of intelligence assessments may go on to re-draft or re-represent the assessment (for example, to abbreviate it for a more senior con-summer or indeed the general public) and thereby lose or misrepresent the sense of the original assessment.

"If intelligence is to be used more widely by governments in public debate in future, those doing so must be careful to explain its uses and its limitations". The Butler Review

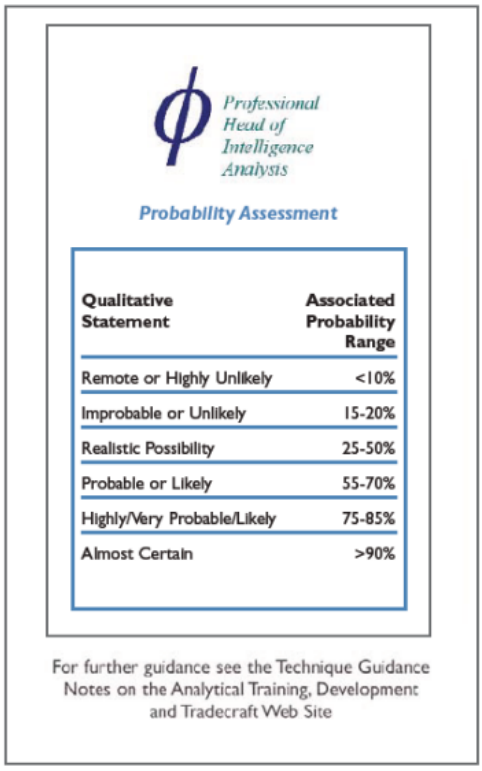
THE UNCERTAINTY OF THE YARDSTICK

A6. In response to the challenges set out above, DIAS mandates the use of a standardised lexicon of terms — The Uncertainty Yardstick — rushing probability and uncertainty.

A7. It assumes familiarity with the basic concept of probability and uncertainty (i.e., what it means to say something like speech marks 'it is 25% likely that RED has an active nuclear programme'.) It also assumes that the analyst has arrived at a probabilistic judgement using a robust method.

A8. As this table suggests, if you believe that a certain hypothesis is 75% likely you should describe it as 'very probable' or 'highly likely'. Clearly, a standardised approach to probabilistic language is only useful so long as readers of our assessments understand it. Consequently, all DIAS products which use the Yardstick should reproduce it, ideally near to the 'Assessment Base' and 'Methodology Boxes.

A9. You will note that the yardstick appears to have gaps ('what about 72%?') This is a deliberate decision to avoid a false impression of accuracy. If your assessment is robust enough to make a fine-grained distinction between 70% and 72%, then it probably makes sense simply to state the figure itself.



Professional Head of Intelligence Analysis

Probability Assessment

Qualitative Statement	Associated Probability Range
Remote or Highly Unlikely	<10%
Improbable or Unlikely	15-20%
Realistic Possibility	25-50%
Probable or Likely	55-70%
Highly/Very Probable/Likely	75-85%
Almost Certain	>90%

For further guidance see the Technique Guidance Notes on the Analytical Training, Development and Tradecraft Web Site

ASSESSMENT FIRST, LANGUAGE SECOND

A10. you should ensure that your assessment of probability comes first, and then the language is chosen (from the Yardstick) to align with the assessment. Doing it the other way around — in other words deciding that something 'feels like' a 'realistic probability' and deciding it's there for 25-50% likely is not a robust method of arriving at a probabilistic judgement.

ALTERNATIVES TO THE YARDSTICK

A11. there are only a few circumstances in which use of the Yardstick is inappropriate. These would include, for instance, an assessment in which the conclusion is sensitive to the difference between 'one and three' and 'one in two' (or 33% and 50%), in a way that the Yardstick cannot capture (both would be scribed as 'realistic possibilities'). If the Yardstick is not sufficiently gradated to capture the details of your assessment, then it is very important to state that alternative lexicon you are using in its place.

PROBABILISTIC LANGUAGE IN OTHER PRODUCTS

A12. The Yardstick is not based on any external standard of probabilistic language. Instead it is a standard that aligns to some extent with survey data on how readers tend to interpret such terms. Although other organisations sometimes use standardised interpretations of probabilistic terms, there is no guarantee they will correspond to those in the Yardstick.

PRECISION ABOUT TIMEFRAME

A13. Another important aspect of communicating judgements concerning uncertainty is to make sure the parameters of the judgement are stated explicitly. Statements about the future should clearly state the

Location: South Mill Road, Amesbury, SP47HR. UK I. Mobile: +44 (0)7742 569943 I Email: frank@cannonassetprotection.uk I Website: https://thecapway.com/

timeframe of the judgement (e.g. , say '2020' rather than the 'long term')

CONDITIONAL PROBABILITIES

A14. You also need to be very clear when you are expressing conditional probabilities – in other words, probabilities of an event occurring given that some other event has already occurred.

For example:

If RED invades ORANGE, there is a realistic possibility that retaliation will involve the use of chemical weapons.

A15. Makes clear that the judgement about ORANGE's use of chemical weapons only applies to the circumstance of an invasion by RED, leaving open the possibility of other circumstances in which chemical weapons might be used.

MODAL LANGUAGE

A16. You should always avoid so-called 'modal' language in the context of a probability judgement. This includes terms such as 'can', 'could', 'might' and 'may', but also 'possible' (except in the form 'realistic possibility'). These are sometimes used as the probabilistic equivalent of 'weasel words': they appear to make a judgement about probability, but all they do in fact is state that something is not impossible, which could imply a probability of 1% or 100%.

A17. Of course, terms such as 'may' and 'could' do serve an important purpose by reminding the reader that something is possible. For example:

RED could withdraw from the NNPT within four months.

A18. There is no reason to avoid them in this context. But analysts should avoid disguising statements about mere possibility as probability judgements, for example:

RED could choose to mount punitive operations against ORANGE facilities, which might prompt an escalation to non-conventional warfare, possibly involving…

AVOIDING FALSE PRECISION

A19. One common argument against the use of a standardised interpretation of probabilistic language is that it is impossible to be sufficiently precise when making judgements about inherently unpredictable events in the political or military sphere. But this is an argument in favour either of improving our methods of making such assessments, or of being explicit about our lack of information. If you have no idea of the probability of an event, then making statements such as:

President Jones will probably try to extend his term of office in 2010.

A20. These will give a misleading impression of precision. It would be more accurate in these circumstances to say:

President Jones might try to extend his term of office in 2010, but we do not have sufficient insight into his decision-making to judge how likely this is.

'CONFIDENCE' AND PROBABILITY

A21. The relationship between confidence and probability is a minefield of possible confusion. The

word 'confidence' is sometimes used as a synonym for probability when making judgements about the likelihood of hypotheses, as in:

We are very confident that RED has an active nuclear programme.

This probably means no more than:

RED is highly likely to have an active nuclear programme.

A22. However, 'confidence' is sometimes also used to express an analyst's judgement about the overall robustness of their assessment, as in:

We are moderately confident in our judgements about RED's technical capabilities, but less so in our judgements about their intentions.

A23. The possibility of confusion is compounded by the fact that other organisations actively recommend using confidence-based terms to express probabilities. However, DIAS recommend that 'confidence' is *never* used as a term expressing probability, whether it is the probability that a hypothesis is true, or the probability of an event occurring: instead, the Yardstick terms are the preferred lexicon. In addition, if analysts recognise that the information underlying an assessment has flaws, it is better to *incorporate* this into their stated probabilities (essentially by downgrading them) and to outline the reasons either in the text or the Assessment Base and Methodology Boxes. So, for example, we do *not* recommend having statements that discuss confidence and probability separately such as:

We have very limited confidence in our judgements about President Jones's intent and decision making.
and

President Jones is almost certain to amend the constitution this year to extend his term of office.

A24. Instead, you should consider that, if our knowledge of Jones's desires is indeed limited, the term 'almost certain' is probably misleading. You might therefore want to consider something closer to the following:

Our knowledge of Jones's intent and decision making is based on fragmentary intelligence from sources on the periphery of his network of advisers.

and

President Jones is likely to amend the constitution this year to extend his term of office.

This better reflects our lack of knowledge about Jones.

AVOIDING INSTITUTIONAL BIASES

A25. Your assessments should be guided only by the strength of the evidence. You should never change your assessments because of pressure to make something more readable or attention-grabbing, or to compensate for a perceived lack of interest among customers. Similarly, do not describe something as more uncertain than it actually is, in response to a concern that you may be subject to scrutiny if it does not occur r proves to be false. For example, if the evidence suggests that an outcome is almost certain, there is still potentially a one-in-ten chance that it won't occur. You should not therefore change your assessment from 'almost certain' to (for example) 'probable' on the basis that if the event does not occur, they will appear 'less wrong'.

A26. The Professional Head of Intelligence Analysis in the Cabinet Office will strongly defend analysts' impartiality in matters such as these. For the analyst's part, it is essential that the evidential basis for all assessments is available, either in released products, or in an evidential audit trail that can be called upon if necessary.

ANNEX B: DELIVERING EFFECTIVE ANALYSIS – COLLEGE OF POLICING

Downloaded on 11 Apr 23 by Frank Cannon: [Delivering effective analysis | College of Policing]

EFFECTIVE ANALYSIS

B1. To assist decision makers, analysts must deliver effective analysis that can be understood and acted upon. One model that illustrates the role of analysis in policing is the '3i model' (Ratcliffe 2004).

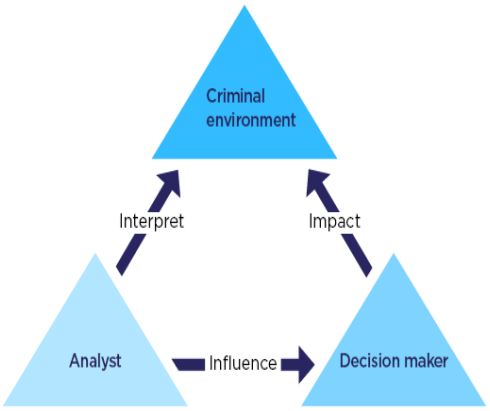


Figure B1: A triangle showing the relationship between Criminal environment, decision maker and analyst.

B2. This model positions the role of the analyst as interpreting the criminal environment, to then influence the decision maker, who will then impact the criminal environment. The value of analysis within this model is therefore in:

a. interpreting the environment, the stage completed within analysing the problem.
b. influencing decision makers by producing work that can be understood and acted on.
c. impacting the environment, completed by the decision maker but informed by translating the work the analyst produces into action.

WRITING FOR IMPACT

B3. The look and feel of an analyst's product is important. The quality and standard of production will make an impression on those who receive it. It is important that all products aim to achieve the best standard in order to command respect, foster trust and have the analytical work acted on.

ABC

B4. Accuracy – analysis should be accurate – factual errors are not acceptable and will undermine analytical products.

B5. Brevity – analysis should be clear, short and to the point.

B6. Clarity – the reader should be able to understand the facts that are presented.

BOTTOM LINE UP FRONT

B7. Bottom Line Up Front (BLUFF) is a good technique to use when producing written and verbal assessments. This is a technique whereby the analyst leads with their analytical conclusion to ensure that, if the customer does not have long to read the product, they will still get an understanding of the key message.

B8. Analysts should follow their conclusion with the supporting evidence, from the strongest to the weakest, ensuring that it contains the 'what', 'so what' and 'what's next' where necessary. Writing in this format ensures that the customer does not need to read the whole document in order to understand the main message. Analysts must believe their bottom line. If not, they should write a new argument.

THE 4-3-3 PRINCIPLE

B9. When writing, analysts should consider using the 4-3-3 (commonly used by the FBI). This should be used as guidance rather than as a fixed rule, as it is not always possible to follow. This principle states that:

a. no sentence should be longer than four lines.
b. no paragraph should be longer than three sentences.
c. no section should have more than three paragraphs.

B10. This style of writing ensures that paragraphs are structured in a way that results in analysts using concise language that is easy to read and understand.

WRITING CLEARLY

B11. When writing reports, analysts should:

a. use clear and unambiguous writing.
b. not make assumptions about the reader's previous knowledge.
c. focus reports on the agreed scope of the terms of reference (TOR).
d. establish confidence in the inferences made by showing the quality of the information sources used.
e. maintain unambiguous and objective reporting (avoiding adjectives such as huge, lacklustre, or significant).
f. invite colleagues to critically read the report to check it is fit for purpose.
g. ensure that enough time remains to complete the report and that it does justice to the amount of analysis/conclusions completed.

KEY FINDINGS AND SUMMARIES

B12. Key findings should be within the scope of the original TOR for the analysis. There should only be six or seven key findings. Each statement should be clear, relevant, and unambiguous. The analysis that supports the key findings should be visible in the text of the final report.

B13. Products such as maps or charts that are more visual in design should be easily understood through effectively presenting the key elements, allowing for more detail to be obtained than through reading any supplementary report or other expanded output.

VISUALISATION

B14. Graphs, tables, pictures, maps, infographics, and other visual methods of presentation can all enhance a product. Indeed, in a visual world, they can form the core of a product, illustrating the relationship between key actors, for example.

B15. It is important to include these only where they add value and to consider the value and impact of these in each case. There will be occasions where an image or other visual aid will be more effective in communicating a message to the reader than a volume of text.

B16. Tables, spreadsheets, and matrices are a useful tool for arranging large amounts of information. They can be used in the collation process and to develop complex charts at a later stage in the analysis. This might include using a table to illustrate sequences of events over a long period, where visual illustration requires too much space or creates too much complexity for the message to be understood.

B17. Maps can help illustrate patterns of movement or demonstrate the relationship between different events. Various data can be overlaid onto maps to support this such as:

a. cell-site data
b. Automatic Number Plate Recognition (ANPR) data
c. points of interest such as home addresses
d. locations of other key sites

B18. Hot spot analysis relies on using maps in particular to illustrate patterns of crime. In this context, it is important to choose the right type of visualisation in analysis and subsequently to illustrate the message, (examples could include point data, kernel density estimation, choropleth mapping or a mixture of these).

B19. 'Infographics' are increasingly employed and can be an attractive and engaging medium for communicating analysis, with key points reinforced by impactive visuals. It can be highly effective in communicating a message and can provide a high level of creative licence to the analyst.

B20. There are many different types of infographics produced and it is a good idea to research examples to identify ideas for a style suitable to the subject matter. By setting out the key message or argument of the analysis (possibly as a 'strapline') and building the rest of the infographic to support this, an analyst can set out their work in a clear and persuasive manner.

B21. Depending on customer requirements, an infographic could accompany a formal written report, or replace it altogether. In the latter case, however, it becomes even more important to design a way of capturing research and analysis that doesn't appear on the infographic in case it is needed to answer questions about the work or in the future.

COMMUNICATING PROBABILITY

B22. Accurately communicating probability is an important element of good-quality intelligence assessment. The agreed standard for conveying probability in intelligence analysis in the UK is the 'PHIA[4] probability yardstick'. This is a scale of probabilistic language developed by Defence Intelligence and latterly adopted by the PHIA for use across the government intelligence community. The scale comprises accepted intelligence terminology at a national level.

B23. This scale demonstrates broad ranges of certainty or uncertainty that can be translated into consistent language. This language is then used in intelligence products in the context of any assessment, accompanied by the scale as an appendix to support interpretation.

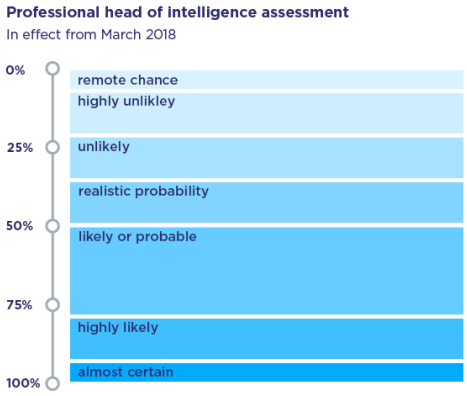
[4] *Inserted by Frank*: The Professional Head of Intelligence Assessments (PHIA). team is responsible for maintaining the professional standards of both analysts and their assessment products, through the Intelligence Analysis Professional Development Framework. Tools such as the PHIA Yardstick and our Common Analytical Standards help ensure that the work of the UK's Intelligence Assessment community meets a consistently high standard and is easily understood by customers.

PHIA PROBABILITY YARDSTICK TABLE

Probability range	Judgement terms	Fraction range
≤ ≈ 5%	Remote chance	≤ ≈ 1/20
≈ 10% to ≈ 20%	Highly unlikely	≈ 1/10 to ≈ 1/5
≈ 25% to ≈ 35%	Unlikely	≈ 1/4 to ≈ 1/3
≈ 40% to <50%	Realistic possibility	≈ 4/10 to < 1/2
≈ 55% to ≈ 75%	Likely or probably	≈ 4/7 to ≈ 3/4
≈ 80% to ≈ 90%	Highly likely	≈ 4/5 to ≈ 9/10
≥ ≈ 95%	Almost certain	≥ ≈ 19/20

Table 1 Key: ≈ approximately equal to. ≥ is greater than or equal to. ≤ is less than or equal to. < is less than

PHIA Probability Yardstick Diagram



B24. This consistent terminology also follows the national intelligence model (NIM) approach to common terminology and operating principles, whereby end users can expect to pick up an intelligence product from any individual in any force or agency and reliably know what the assessment is seeking to communicate around the certainty or otherwise of any judgements.

B25. For further information, see PHIA Analysis Guidance (opens an external website in the same tab) (available to authorised users logged on to the restricted online College Learn (opens an external website in the same tab)).

B26. The scale was developed in response to two key challenges to effective intelligence assessment, namely the potential for:

a. misinterpretation – a lack of consistency in the use of language means that the same terms can be used to describe very different things, meaning that the findings of any assessment could be wrongly interpreted and therefore improperly acted on

b. misrepresentation – vagueness through a lack of consistency can lead to an intelligence assessment being accidentally or deliberately misrepresented by the end user, particularly if the work is quoted or collated into another product, potentially leading to inappropriate action.

WRITING FOR ACTION

DEVELOPING RECOMMENDATIONS

B27. A clear set of recommendations should be included in analytical reports. These should be based on the analysis and focus on key findings or information gaps relevant to the issue being analysed.

B28. Recommendations should be written as directional statements and be limited to perhaps six or seven of the key issues. Recommendations should follow a structure, such as SMART, where any recommendation is:

a. Specific – recommendations should be clear, detailed, and unambiguous.

b. Measurable – recommendations should make it clear exactly what needs to be achieved. They should help to set operational objectives and objectives for results analysis.

c. Achievable – all recommendations should be achievable and focused on what can be done with available resources.

d. Realistic or relevant – the recommendations should be within the scope of the original TOR for the analysis and be realistically achieved if adopted.

e. Timely – recommendations should be presented as short, medium, or long-term options. Alternatively, they could be prioritised and given a schedule.

B29. Analysts may make recommendations across a range of issues. This stage of the analysis may require analysts to engage with other analysts, researchers, or other intelligence professionals, with operational specialists or with subject matter experts and to jointly deliver any recommendations, as required.

CHECKLIST FOR REPORT WRITING

The key points to consider when developing a report are:

1. only develop key findings, information gaps and recommendations once the analysis is completed.
2. write up the analysis before developing the key findings, information gaps and recommendations to ensure that they follow a standard and logical order of presentation.
3. once the analysis is written up, highlight the points that are to be communicated as key findings, and where the analysis suggests further action.
4. discuss the analysis with an experienced colleague who may assist in identifying the most important findings from the analysis.
5. use the collection plan to identify the information that was not received or found and assess the impact of that gap on the findings.
6. consider what should be added to the TOR or done if there was more time or information and whether this would improve the task that was set, or operational activity.
7. if so, consider including the information as recommendations.
8. write recommendations in the analysis as a first step to ensure that they are supported by the analysis and evidenced in the text – they can then be moved to the appropriate section of the report.
9. use the review process (see below) to check that the key findings, information gaps and recommendations are unambiguous, clear, and directly relevant to the TOR.

PROBLEM SOLVING

B30. Analysts within certain functions may take a direct role in operational activity related to their work, particularly in areas relating to volume crime or antisocial behaviour. This might include taking part in problem-solving activity.

B31. Problem solving[5] is supported by analysis and is best achieved by adopting a collaborative approach. Collaboration should include subject experts (in crime prevention, neighbourhood teams, forensic staff, analysts, investigators, intelligence staff and partners) and, where relevant, a trained facilitator or someone outside the group to run problem-solving meetings or workshops.

B32. Prior to meeting, all those involved must have read the analysis report or intelligence product. Researching best practice resources such as the College of Policing website for possible responses prior to the meeting can also be beneficial in understanding what has previously been used to counter similar problems. Also consider using organisational memory databases in force and results analysis reports. Any collaborative sessions may also benefit from using appropriate analytical techniques, including hypotheses generation and testing, SWOT, structured brainstorming, or key assumptions checks.

GOING BEYOND THE DESCRIPTIVE

B33. The value of analysis will most often be realised when the product provides an assessment that delivers insight, clarity, and context. The purpose of the product will have been established through the TOR stage. Where a product is required to go beyond the descriptive, to explain why something has happened, to evaluate what something means or to estimate what might happen next, the analyst must add value (Pherson and Sullivan 2013).

B34. Value may be added by using appropriate analytical techniques to make inferences, to generate and test hypotheses or to develop scenarios as required. It is important to communicate these and subsequent findings and conclusions effectively. Going beyond the descriptive should increase the potential for action to be taken by identifying actionable lines of enquiry, intelligence gaps or intelligence indicators.

QUALITY REVIEW

B35. Once the product is complete, review is a key step to establish that the product is clear and concise and responds to the original TOR. Reviews take a number of formats including:

a. peer review by a colleague.
b. formal or informal quality review by an analyst manager.
c. stakeholder reviews by those commissioning the work.

B36. The review might represent a planned milestone in producing the work or may be done prior to accepting the completed work. Stakeholders might include partners as diverse as the Crown Prosecution Service (CPS), for work presented in court, partner agencies for joint strategic or tactical products or government agencies which have tasked work out to forces.

B37. Analysts should confirm that:

a. the TOR have been achieved.
b. inferences and key findings are the correct ones.
c. findings are supported by the report text.

[5] The underlined text was an active link to further information within the College of Policing website; these links have not been copied into this paper.

B38. When planning the timescale for producing analysis, adequate time should always be built in for review. It is important to provide the reviewer with the TOR so that they are aware of what the analysis is trying to achieve and can check that any specific questions are fully answered. When seeking peer review, the analyst should choose a colleague able to provide an objective view.

B39. Examples of the questions that the reviewer should answer include the following.

a. Are the key findings clear?
b. Does the work add value, providing insight, clarity, context, or direction, for example?
c. Does the document make sense?
d. Does it read well?
e. Does the reviewer agree with the findings based on the content of the document?
f. Do the arguments make sense?
g. Do the key findings support the inferences and the core argument(s)?
h. Did the analyst make use of appropriate analytical tools and techniques?
i. Do the recommendations flow from information gaps and key findings?
j. Are relevant minimum standards complied with?
k. So what? What does this work achieve? What does it say, enable or inform?

B40. The reviewer should give honest, constructive feedback, and the originating analyst should receive the feedback in such a light. If the answer to any of the questions listed is 'no', then the originating analyst may like to consider amending the way the information is presented. The most effective way of exchanging feedback is to ask the reviewer to brief the originating analyst directly, enabling clarification of any feedback and discussion of changes suggested. Any changes can then be made immediately without delaying dissemination of the product and without altering the authorship and analytic line of the product.

DISSEMINATING ANALYTICAL OUTPUT

B41. Dissemination should be agreed and set out in the TOR. Consideration should be given to who needs the information and the most appropriate format for dissemination. The amount of information disseminated will vary, depending on the audience. For one audience it may be appropriate to provide detail of the analysis. For others, it may be more appropriate to provide only the intelligence gaps and give direction on how they might be filled.

B42. The analyst is responsible for producing and disseminating appropriate material. They should ensure that products are version controlled and comply with the corporate style and any minimum requirements. This ensures a professional approach and supports continual improvement of future work.

B43. Specifically, the analyst must ensure that the:

a. Correct Government Security Classification (GSC) grading is considered and properly shown.
b. Document is being disseminated in accordance with the GSC.
c. Most appropriate media for dissemination is chosen.
d. Recipient is able to access the report and has the software necessary to read attached charts or maps.
e. Recipient is aware of any restrictions on the storage of the report.
f. Original report is stored correctly and is easily accessible in the future.
g. Briefings and presentations are often used by analysts to supplement written reports.

B44. They may also be used in the place of written reports to disseminate results to some audiences. Good presentation and briefing skills are an important part of an analyst's skills and abilities. Some key elements to remember for preparing and giving briefings and presentations are:

a. know the material and be prepared for questions.
b. keep it brief and keep to allotted time.
c. focus on three or four key messages.
d. keep supporting slides to a minimum (don't read them).
e. use charts and maps to support the content.
f. know the audience and pitch accordingly.
g. avoid fidgeting and standing with hands in pockets, or arms folded in front of the body and use open body language.
h. maintain eye contact, breathe, and smile.

CHECKLIST – DISSEMINATING ANALYSIS

1. The key points to consider when disseminating analysis are:

2. Identify barriers to dissemination early on in the analysis process and assess the risk of not removing them.

3. Follow the dissemination requirements set out in the TOR.

4. Check that the GCS is correct and is appropriately displayed on the report and supporting media.

5. Keep a list of the recipients of the report and consider asking them for feedback if this is not done automatically.

6. Ensure that deadlines are adhered to by leaving time to check that the customer has received the report and that any consultation processes have been followed.

Location: South Mill Road, Amesbury, SP47HR. UK I. Mobile: +44 (0)7742 569943 I Email: frank@cannonassetprotection.uk I Website: https://thecapway.com/