FIU | Jack D. Gordon Institute for Public Policy
Steven J. Green School of International and Public Affairs

NCTC Threat Analysis Simulation

Homefront:
Radicalization in America

Preparation Materials

FIU | Kimberly Green Latin American and Caribbean Center

Miami-Dade County Public Schools
giving our students the world

ICCAE
Intelligence Community Centers for Academic Excellence

Disclaimer

* The following active learning product is based on various articles journals. Please see the references section for more information. Liberties are taken with the background information, scenario and circumstances to make the activity useful and accessible to students and educators. Therefore, the following activity is not entirely factual or entirely fictitious. It is a simulation that takes cues from current events, but constructs an "alternate reality" fit for an educational setting. Please do not be misled if there are aspects of the exercise that are not entirely consistent with recent developments involving ISIS, U.S. counterterrorism efforts, and other actors involved in the exercise.

** All materials herein are presented for educational purposes by its designers, and do not reflect the views or opinions of Florida International University and the Jack D. Gordon Institute for Public Policy, nor of the United States Government. The views, opinions, and/or findings contained in this document are those of the author(s) and should not be construed as an official position, policy, or decision unless so designated by other official documentation.

***Cover Photo Right: Omar, Ammar Cheikh, and Cassandra Vinograd. "ISIS Anniversary: The Year Since Caliphate Was Declared." NBCNews.com. June 29, 2015. Accessed September 29, 2017. https://www.nbcnews.com/storyline/isis-uncovered/isis-anniversary-year-caliphate-was-declared-n381621.

**** Cover Photo Left: FBI. "Partnerships." May 03, 2016. Accessed September 29, 2017. https://www.fbi.gov/about/partnerships.

Author & Lead Researcher: Tyler McDaniel

Researcher: Jessica Viteri

Editors: Hector Cadavid; Aldo Fonseca

TABLE OF CONTENTS

INTRODUCTION

Crisis Decision-Making and the National Counterterrorism Center

Following the attacks of 9/11, the United States intelligence community (IC) was forced to realize the real and mortal threat that international terrorism posed to American lives and interests. The IC was restructured to correct the systematic oversights within, and to reorient national security organizations to deal with attacks upon the homeland by non-state actors.

The NCTC Threat Analysis Simulation is a dynamic exercise designed to highlight the challenges of crisis decision-making within this new intelligence environment. The threats posed by individuals waging terrorist attacks in the United States has been impossible to ignore with recent ISIS-inspired attacks in recent years. Crisis management simulations such as this are meant to portray the real work being done by counterterrorism intelligence officers on behalf of the United States.

The **Jack D. Gordon Institute for Public Policy Program in National Security Studies** offers today's exercise for you to learn about the complexity of executive decision-making, especially in crisis situations that can potentially endanger the lives of millions. As analysts assigned to the NCTC crisis taskforce, participants will carefully consider possible outcomes within their agency groups in addition to their inter-agency groups and what the implications to sovereign security may be. We hope the simulation will inspire a greater appreciation for international politics and motivate your interest in National Security Studies.

BACKGROUND

Mission of the National Counterterrorism Center

More than a decade following 9/11, the threat of a terrorist attack within the United States is a persistent and ever-changing one. To combat these potential risks, the Federal Government has modified sections of the intelligence community (IC) and created entirely new organizations charged exclusively with assessing such threats. One of these organizations is the National Counterterrorism Center (NCTC). NCTC's mission statement is stated as follows:

> *"We lead and integrate the national counterterrorism (CT) effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure our national CT objectives."*[1]

NCTC's scope is very wide with responsibilities that range from the creation and dissemination of vital and relevant terrorist threat information to all members of the United States' intelligence community to developing guidance products to inform and train first responders how to spot and respond to a terrorist incident in municipalities throughout the nation.

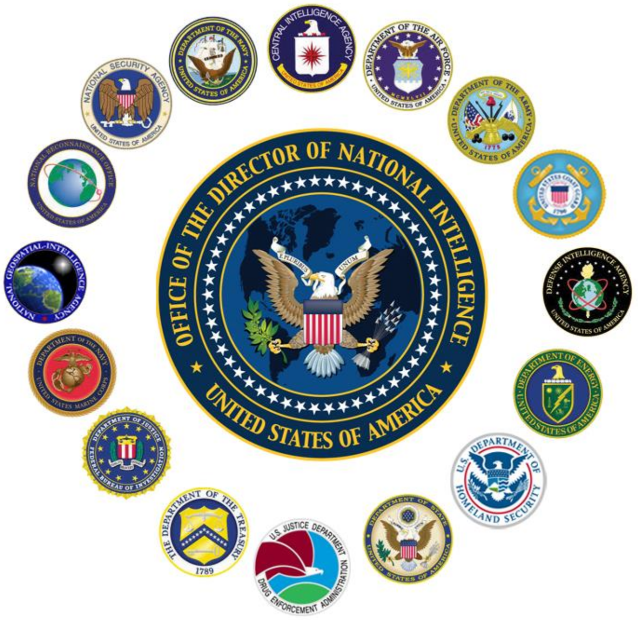


Figure 1. The agencies that make up the U.S. Intelligence Community Source: Wikipedia (https://upload.wikimedia.org/wikipedia/commons/9/9b/IC_Circle.jpg)

Origins of the National Counterterrorism Center

NCTC's creation can be said to be as a result of the attacks on 9/11 and the investigation following it. This investigation found the United States intelligence community unable to "connect the dots" and see the potential threat of a terrorist incident on U.S. soil.[2] A smokestack effect where pieces of intelligence that, by themselves, tell nothing important but together, paint a picture of the imminent threat was a major factor in this intelligence failure. This, coupled with a failure of imagination on the part of intelligence analysts, is often claimed to be the deciding factors in the United States' inability to predict the events of 9/11.[3]

The Office of the Director of National Intelligence (ODNI) was created as a result of these conclusions and aims to mitigate these pitfalls by being an umbrella organization that enables and encourages the sharing of intelligence between U.S. intelligence agencies while ensuring intelligence security. NCTC, as part of the ODNI, fulfills this role within the context of terrorist threats.

[1] "Who We Are." ODNI: NCTC. Accessed May 30, 2017. https://www.dni.gov/index.php/nctc-who-we-are.

[2] Burch, James. "The Domestic Intelligence Gap: Progress Since 9/11?" Homeland Security and Affairs: The Journal of the NPS Center for Homeland Defense and Security. January 23, 2015. Accessed May 30, 2017. https://www.hsaj.org/articles/129.

[3] Russell, Alec. "9/11 Report Condemns 'failure of Imagination'." The Telegraph. July 23, 2004. Accessed May 30, 2017. http://www.telegraph.co.uk/news/worldnews/northamerica/usa/1467701/911-report-condemns-failure-of-imagination.html.

NCTC's Organization and Structure

Threat Analysis

NCTC acts as the primary organization for analysis and integration of all intelligence pertaining to terrorism and counterterrorism. In this role, the NCTC has the responsibility to inform all of its partners of pertinent information on all terrorist issues and to analyze intelligence given to them from those same partners.[4]

> *"NCTC serves as the primary organization in the US government for analyzing and integrating all intelligence possessed or acquired by the government pertaining to terrorism and [counter terrorism] […] NCTC also leads interagency task forces designed to analyze, monitor, and disrupt potential terrorist attacks."*
>
> "NCTC at a Glance" – dni.gov

Strategic Operational Planning

NCTC also conducts strategic planning for counterterrorism activities across the US government. Integrating a wide variety of intelligence from sources such as military, diplomatic, financial, and law enforcement, NCTC is able to provide a more complete situational and tactical picture to aid in counterterrorism operations. For this reason, NCTC leads interagency taskforces designed to analyze, monitor, or disrupt potential terrorist attacks.[5]

Identity Management

Another vital role that NCTC plays is its management of a shared knowledge bank on known and suspected terrorists and international terror groups, as well as their goals, strategies, capabilities, and networks of contacts and support. This knowledge bank is called the Terrorist Identities Datamart Environment (TIDE). This classified repository lists names, dates of birth, biometric information, photos, and information explaining the subject's link(s) to terrorism. TIDE's information is sourced from resources which include local law enforcement, the Transportation Security Administration (TSA), and the State Department. TIDE acts as a database to support screening activities as well as an analytic tool in NCTC's effort to assess terrorist threats.[6]

The NCTC Operations Center

One way the NCTC fulfills its role in assessing terrorist threats globally and domestically is its creation and maintenance of the NCTC 24/7 operations center.[7] Here, pieces of intelligence from local law enforcement, open-source media, and the national intelligence community are submitted and collated into intelligence products for NCTC's many customers who include the Director of National Intelligence, the President of the United States, all members of the United States Intelligence Community, and local authorities and first responders.

[4] "NCTC At a Glance." Office of the Director of National Intelligence 119, no. 2 (February 01, 2011). Accessed May 30, 2017.

[5] Ibid.

[6] Ibid.

[7] "What We Do." ODNI: NCTC. Accessed May 30, 2017. https://www.dni.gov/index.php/nctc-what-we-do.

Figure 2 NCTC Operations Center

Within the NCTC's operations center are intelligence professionals "on loan" from the many agencies within the IC. These professionals retain the rights and privileges of their respective roles in their home agencies as a means to cut through bureaucratic red tape that can often impede efficient sharing of vital information to the NCTC's customers.

These intelligence professionals comb through numerous bits of data from the NCTC's wealth of resources in an attempt to unearth an indication of a potential terrorist threat.[8] The form that this intelligence takes is what is sometimes called a feed; single pieces of information that may be important to their CT activities. The analysts use the various resources at their disposal to confirm or refute other pieces of intelligence to build an analytical line of thought to communicate to their customers.

However, NCTC, like many other analytical bodies within the IC, does not have operational authority; that is, they do not perform counterterrorism (CT) operations themselves. NCTC primarily identifies and assesses terrorist threats and makes recommendations to its customers as to a beneficial course of action.

[8] Marks, Alexandra. "Spending a Day at the National Counter Terrorism Center." The Christian Science Monitor. June 13, 2007. Accessed May 30, 2017. http://www.csmonitor.com/2007/0613/p20s01-ussc.html.

The American Intelligence Community

The following is a brief overview and mission statement of the select intelligence agencies included in this simulation. Participants should be aware of the jurisdiction and permissions of their particular agency.

Department of State

The Department of State (DOS) is the lead agency for U.S. foreign policy and diplomacy. Its intelligence support component is the Bureau of Intelligence and Research (INR). The U.S. was the first federal executive department established and it is led by the Secretary of State who is nominated by the POTUS and confirmed by the Senate.

Mission Statement:

The Department's mission is to shape and sustain a peaceful, prosperous, just, and democratic world and foster conditions for stability and progress for the benefit of the American people and people everywhere. This mission is shared with the USAID, ensuring we have a common path forward in partnership as we invest in the shared security and prosperity that will ultimately better prepare us for the challenges of tomorrow.

Central Intelligence Agency

The Central Intelligence Agency (CIA) was established by former President Franklin D. Roosevelt in efforts to streamline the collection, organization, and dissemination of the intelligence that the government agencies collect. The CIA is the largest producer of all-source national security intelligence for senior U.S. policymakers in the national security and defense arenas. CIA’s information, insights, and actions consistently provide tactical and strategic advantage for the United States.

Mission Statement:

Preempt threats and further US national security objectives by collecting intelligence that matters, producing objective all-source analysis, conducting effective covert action as directed by the President, and safeguarding the secrets that help keep our Nation safe.

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) is an intelligence-driven and threat-focused national security organization with both intelligence and law enforcement responsibilities. The FBI works to protect the U.S. from terrorism, espionage, cyber-attacks, and major criminal threats. The FBI evolved is the investigative force of the Department of Justice. The FBI has jurisdiction over the U.S. and its territory and generally does not have the authority to arrest individuals located outside of the United States.

Mission Statement:

To protect the American people and uphold the Constitution of the United States.

National Security Agency

The National Security Agency (NSA) aims to provide timely and accurate cryptology knowledge, teaming up with senior military and civilian leaders to address and act on critical issues of national and tactical intelligence objectives. NSA is part of the Department of Defense, and is staffed by a combination of civilian and military personnel.

Mission Statement:

The National Security Agency/Central Security Service (NSA/CSS) leads the U.S. Government in cryptology that encompasses both Signals Intelligence (SIGINT) and Information Assurance (IA) products and services, and enables Computer Network Operations (CNO) in order to gain a decision advantage for the Nation and our allies under all circumstances.

Department of Homeland Security

The Department of Homeland Security (DHS) is responsible for leading the unified effort to secure the United States by preventing and deterring terrorist attacks and responding to threats and hazards. The DHS was established in 2002 and it combined 22 different federal departments and agencies into a unified, integrated cabinet agency. The Office of Intelligence and Analysis (I&A) provides intelligence support across the whole range of Homeland Security missions. I&A ensures that information related to homeland security is collected, analyzed, and disseminated to all relevant customers.

Mission Statement:

With honor and integrity, we will safeguard the American people, our homeland, and our values.

Creation of ISIS

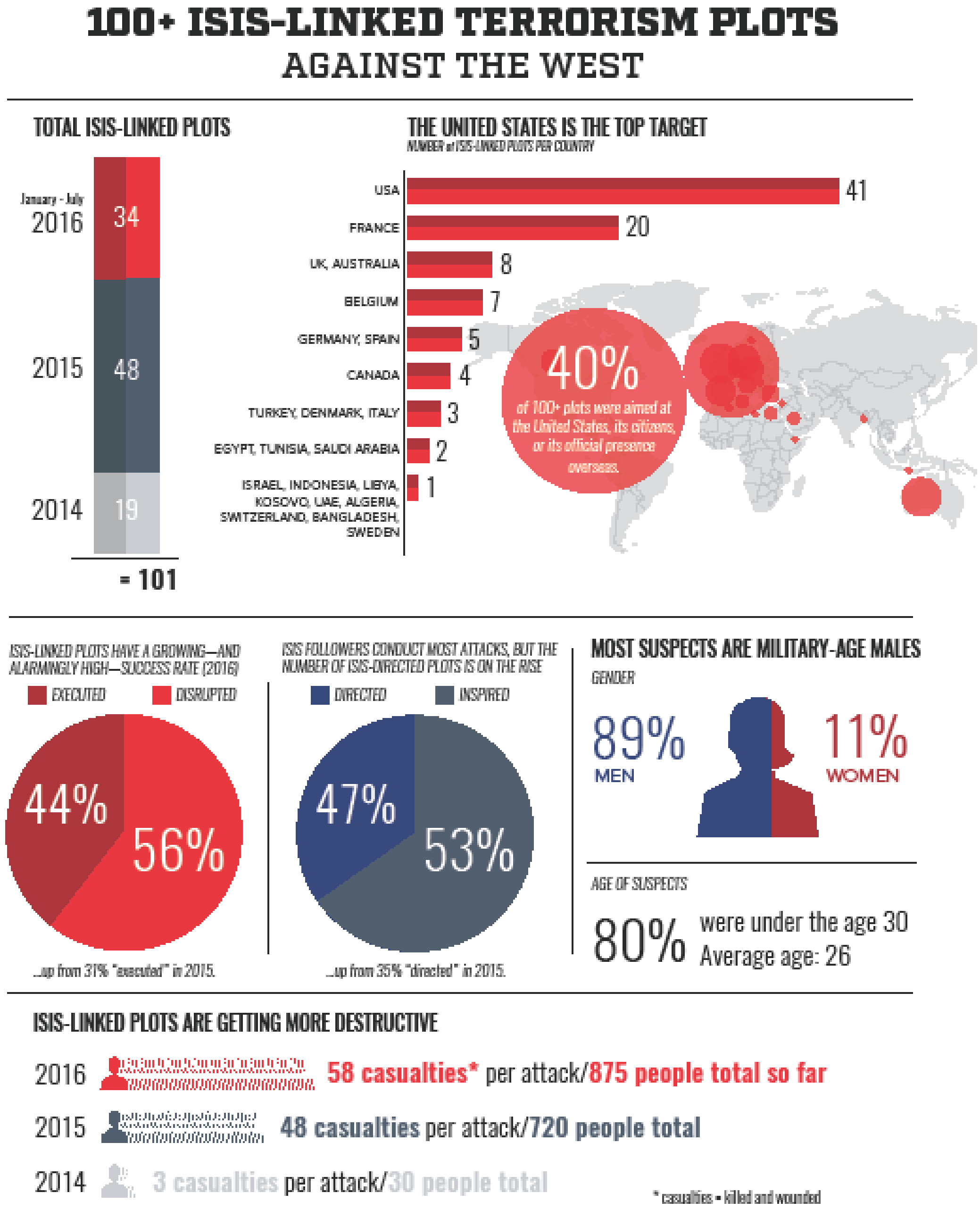
The content of the simulation covers a fictional commissioning of a terrorist act by ISIS upon the West. The following is background on ISIS, its ideology, and its previously utilized methods of radicalization and attack.

ISIS took early form as a branch of Al Qaeda forces from Iraq seeking to put down roots in war-torn Syria where they could operate more comfortably than in Iraq which had seen the results of an American troop surge in recent years. After moving into Syria, this branch branded themselves as The Islamic State of Iraq and Syria (ISIS.) ISIS finally split from Al Qaeda following intellectual and tactical disputes; for example, whether or not Al Qaeda should seek territorial expansion as opposed to exclusively targeting and killing ideological enemies.

ISIS made major gains in the fighting in Syria and was one of the first groups to capture major cities in the civil war. Finally, ISIS waged a successful campaign to capture the Iraqi city of Mosul. Following this successful assault and ISIS's rise in notoriety, other extremist groups in the Middle East and Africa such as Boko Haram pledged their allegiance to the jihadist organization.

ISIS's fame and infamy grew more as a result of their strong social media presence where it attempted to shock enemies of ISIS and recruit fellow Muslims globally to their cause. Often ISIS has posted videos depicting brutal killings of those they have captured. However, in contrast to Al Qaeda, ISIS has attempted to wage a territorial war in the Middle East and simply called on Muslims in the West to join in their fighting in the region.[9] Nonetheless, possibly as a result of anti-ISIS campaigns by multiple nations and groups, the number of attacks in the West claimed to be inspired by ISIS has begun to grow in recent years.

[9] Wood, Graeme. "What ISIS Really Wants." The Atlantic. April 14, 2016. Accessed September 26, 2017. https://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/.



[10]

[10] "What ISIS Really Wants." Digital image. The Atlantic. March 2015. https://cdn.theatlantic.com/assets/media/img/2015/02/17/ISIS_Web_feature2/1920.jpg?1440086852.

Scenario

Overview: Senior policy makers have identified a potential terrorist threat within the United States by a foreign terror organization. Following the identification of this possible threat, senior officials from each respective intelligence agency have created individual ad hoc taskforces to identify specifically the nature of this threat, who the possible individual(s) coordinating the attack may be, and to inform the relevant organizations and/or agencies of necessary details concerning the threat.

The simulation participants will role-play as analysts at several U.S. intelligence agencies and local authorities. Participants will accomplish the goal of their respective taskforces by analyzing the situation on several fronts:

•Describe the possible threat. (Who? What Where? When? How?)

•Explain the specifics of the threat. (Motives. Why?)

•Predict what could happen given their assessment. (How can the situation change? What can the future bring?)

The report that the simulation analysts submit will take form as a result of tasks given to them throughout the simulation. This report will also include an oral brief by the analysts of policy makers and appropriate institutions whom have an interest in the current matter.

Simulation Procedure

Simulation participants will be separated into eight groups of analysts composing five separate taskforces of agencies within the IC and two "local liaisons"; local authorities within the U.S. with possibly relevant intelligence to the current crisis. Each group will be given intelligence packets and asked to answer the same analytical questions.

As each group will be working separately, it is likely that these groups' conclusions and recommended courses of action will differ significantly as the simulation progresses. This is expected and acceptable. Often when analyzing data, many different but suitable conclusions can be drawn. The goal of the simulation is to provide participants insight into analytic methods such as structured analytical techniques. To illustrate these techniques, the simulation will be broken up into three rounds.

The elements of the attack that analysts are looking to determine are:

1. The most probable location.
2. The most probable means.
3. The likely perpetrators.

Round One

After participants are assembled into taskforces of their respective agencies, the analysts will be given an intelligence packet considered relevant to the current crisis. This packet will include a combination of both classified and open-source intelligence. While some information between the agencies will be the same, the majority of the intelligence packets will be composed primarily of information that the individual agencies would have access to. That is, the information in these packets will only include information that each agency would be able to collect or have the privilege to review.

During this round, analysts will read over their packets individually, without collaborating so as to form their first impressions of the situation. Following this, analysts will discuss amongst themselves not only their theory of the potential threat but also where they feel there is a shortage of information and attempt to “separate the wheat from the chaff” in regards to individual pieces of intelligence. In other words, what of the information given seems of higher quality and veracity and what may be erroneous or misleading?

Round Two

At the end of Round One, the analysts will be reorganized into new taskforces organized by the NCTC with all agencies and organization represented within each. During this round, intelligence is shared between the analysts to try to reassess and eliminate less likely theories and hone their consensus towards the most likely.

The new data provided by the interaction of the agencies may or may not change their current assessment and analysts are encouraged to deliberate amongst themselves as to how the situation has developed. Questions analysts should be asking themselves are:

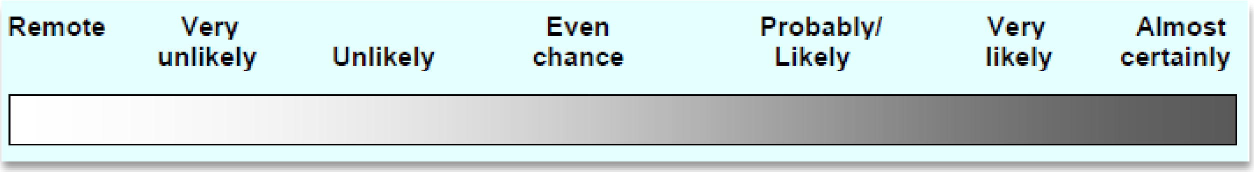
- What hypothesis are we most confident about? What could be the result if we are ultimately wrong about it?
- What are some reasons we could be wrong about our current hypothesis?
- Are we relying too much on selected pieces of evidence?

Round Three

Following Round Two, no new intelligence packets will be distributed. During this round, analysts should be finalizing their analytic judgements and gathering the evidence in support of them. After this finalization, analysts will compose a situation report (‘sit-rep’) to ODNI supervisors and federal decision makers. Here, those leading the brief will inform their customers as to their estimates of likelihood of the terrorist threat, what significant information is unknown, and state with what degree of confidence they hold their conclusions. In addition, teams will state what relevant organizations (public and/or private) need to be informed of their appraisal.

Taskforces should attempt to reach a consensus but it is important that dissenting opinions and viewpoints are not dismissed outright. If fellow analysts disagree as to the opposing conclusions being raised but feel the argument has some merits, it is acceptable and indeed encouraged that other theories be incorporated. However, if a taskforce casts too wide of a net or even resorts to simply restate the content given then this will likely result in a poor quality brief. Decision makers, especially during a crisis of this nature, often do not have extra time for nonessential information. Those creating the briefs should keep this in mind when assembling their reports.

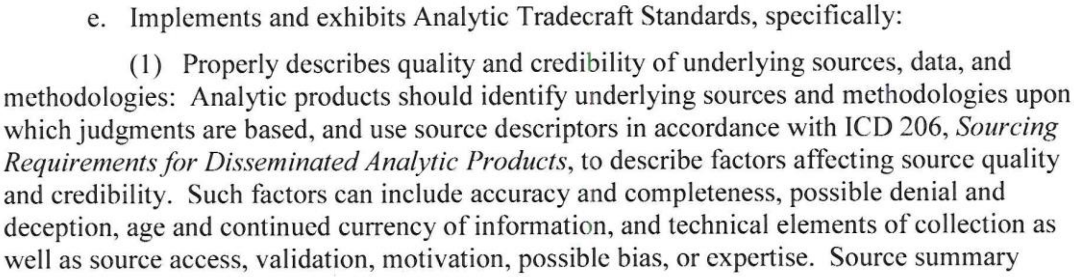
The content of the briefs should attempt to follow the analytic standards described in detail in Appendix A. In short, analysts must be able to relate their conclusions on two fronts: *probability* and *certainty*. Probability describes the likelihood of an event ranging from ‘almost no chance’ to ‘almost certainly.’



Source: Intelligence & Policy

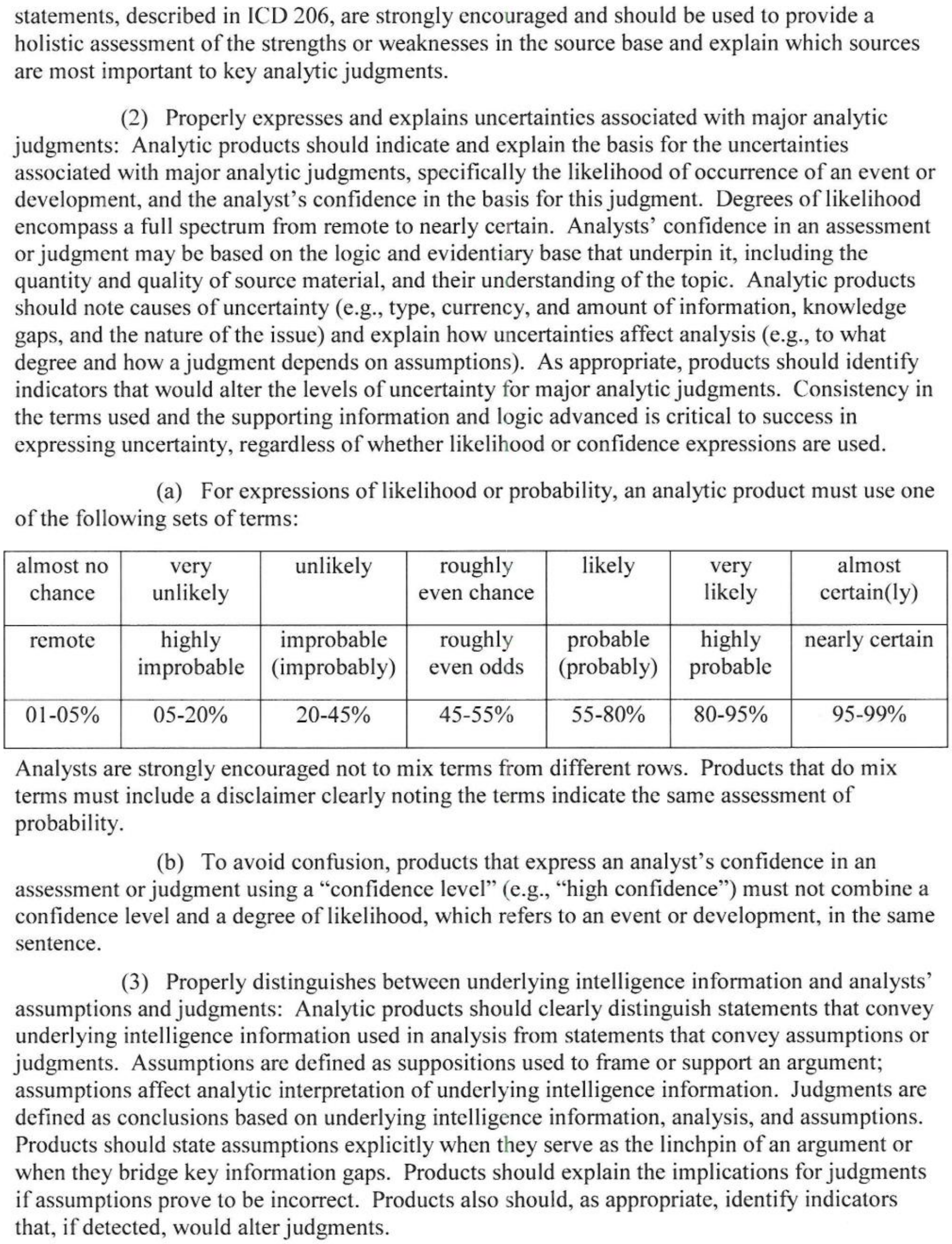
Confidence assessments indicate the credibility of the analysts' sourcing in making their conclusions. These assessments are typically related by stating one has a high, moderate, or low degree of confidence. 'High confidence' indicates the judgements are derived from highly credible sources making the judgement valid. It is important to note that high confidence does not constitute a fact or certainty of an assessment. 'Low confidence' indicates that the sourcing of data from which the analysts' have drawn their conclusions is of low credibility, fragmented, and/or poorly corroborated.

APPENDIX A – Analytic Standards



e. Implements and exhibits Analytic Tradecraft Standards, specifically:

(1) Properly describes quality and credibility of underlying sources, data, and methodologies: Analytic products should identify underlying sources and methodologies upon which judgments are based, and use source descriptors in accordance with ICD 206, *Sourcing Requirements for Disseminated Analytic Products*, to describe factors affecting source quality and credibility. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection as well as source access, validation, motivation, possible bias, or expertise. Source summary



statements, described in ICD 206, are strongly encouraged and should be used to provide a holistic assessment of the strengths or weaknesses in the source base and explain which sources are most important to key analytic judgments.

(2) Properly expresses and explains uncertainties associated with major analytic judgments: Analytic products should indicate and explain the basis for the uncertainties associated with major analytic judgments, specifically the likelihood of occurrence of an event or development, and the analyst's confidence in the basis for this judgment. Degrees of likelihood encompass a full spectrum from remote to nearly certain. Analysts' confidence in an assessment or judgment may be based on the logic and evidentiary base that underpin it, including the quantity and quality of source material, and their understanding of the topic. Analytic products should note causes of uncertainty (e.g., type, currency, and amount of information, knowledge gaps, and the nature of the issue) and explain how uncertainties affect analysis (e.g., to what degree and how a judgment depends on assumptions). As appropriate, products should identify indicators that would alter the levels of uncertainty for major analytic judgments. Consistency in the terms used and the supporting information and logic advanced is critical to success in expressing uncertainty, regardless of whether likelihood or confidence expressions are used.

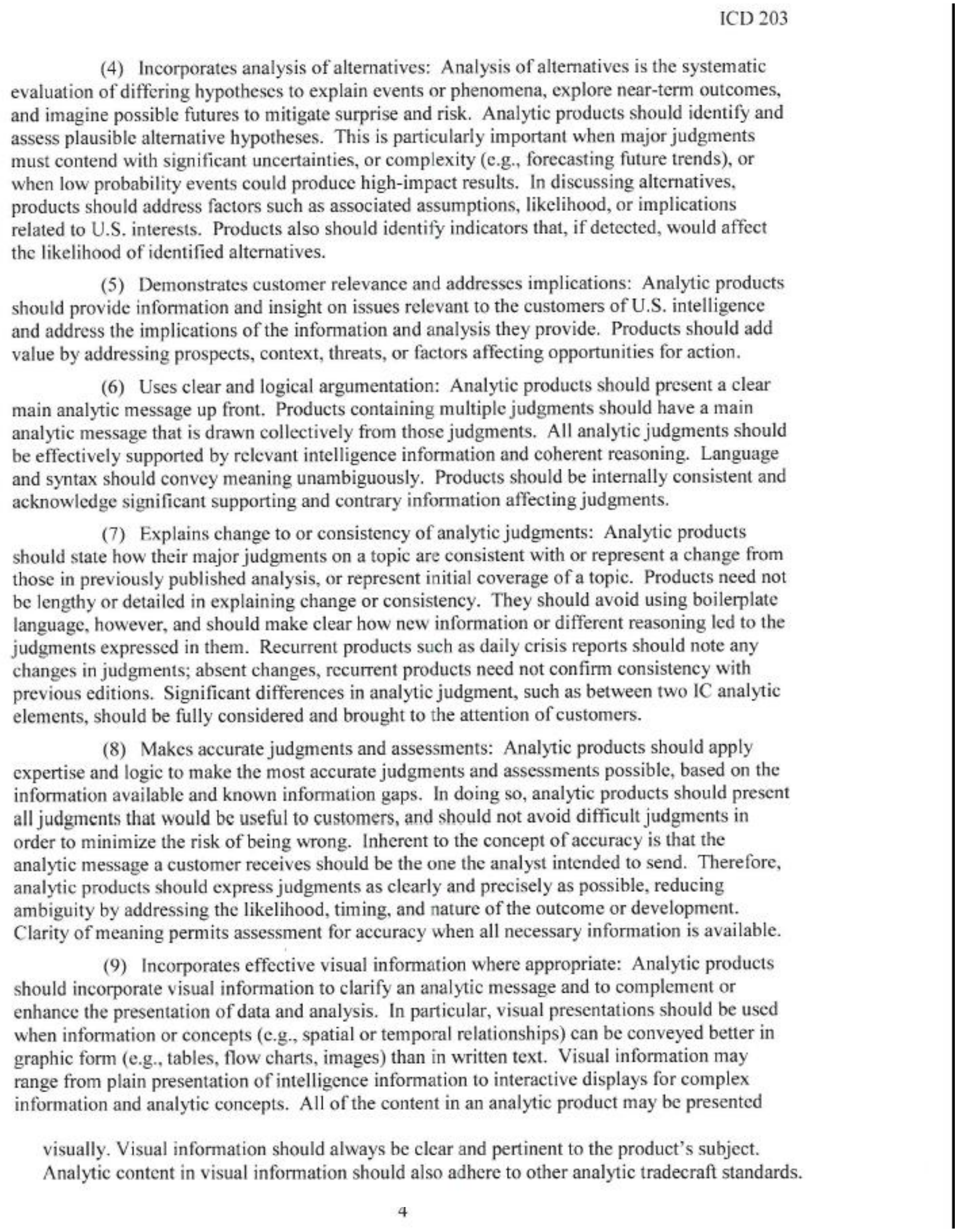
(a) For expressions of likelihood or probability, an analytic product must use one of the following sets of terms:

almost no chance	very unlikely	unlikely	roughly even chance	likely	very likely	almost certain(ly)
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%

Analysts are strongly encouraged not to mix terms from different rows. Products that do mix terms must include a disclaimer clearly noting the terms indicate the same assessment of probability.

(b) To avoid confusion, products that express an analyst's confidence in an assessment or judgment using a "confidence level" (e.g., "high confidence") must not combine a confidence level and a degree of likelihood, which refers to an event or development, in the same sentence.

(3) Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments: Analytic products should clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments. Assumptions are defined as suppositions used to frame or support an argument; assumptions affect analytic interpretation of underlying intelligence information. Judgments are defined as conclusions based on underlying intelligence information, analysis, and assumptions. Products should state assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps. Products should explain the implications for judgments if assumptions prove to be incorrect. Products also should, as appropriate, identify indicators that, if detected, would alter judgments.



(4) Incorporates analysis of alternatives: Analysis of alternatives is the systematic evaluation of differing hypotheses to explain events or phenomena, explore near-term outcomes, and imagine possible futures to mitigate surprise and risk. Analytic products should identify and assess plausible alternative hypotheses. This is particularly important when major judgments must contend with significant uncertainties, or complexity (e.g., forecasting future trends), or when low probability events could produce high-impact results. In discussing alternatives, products should address factors such as associated assumptions, likelihood, or implications related to U.S. interests. Products also should identify indicators that, if detected, would affect the likelihood of identified alternatives.

(5) Demonstrates customer relevance and addresses implications: Analytic products should provide information and insight on issues relevant to the customers of U.S. intelligence and address the implications of the information and analysis they provide. Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.

(6) Uses clear and logical argumentation: Analytic products should present a clear main analytic message up front. Products containing multiple judgments should have a main analytic message that is drawn collectively from those judgments. All analytic judgments should be effectively supported by relevant intelligence information and coherent reasoning. Language and syntax should convey meaning unambiguously. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.

(7) Explains change to or consistency of analytic judgments: Analytic products should state how their major judgments on a topic are consistent with or represent a change from those in previously published analysis, or represent initial coverage of a topic. Products need not be lengthy or detailed in explaining change or consistency. They should avoid using boilerplate language, however, and should make clear how new information or different reasoning led to the judgments expressed in them. Recurrent products such as daily crisis reports should note any changes in judgments; absent changes, recurrent products need not confirm consistency with previous editions. Significant differences in analytic judgment, such as between two IC analytic elements, should be fully considered and brought to the attention of customers.

(8) Makes accurate judgments and assessments: Analytic products should apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps. In doing so, analytic products should present all judgments that would be useful to customers, and should not avoid difficult judgments in order to minimize the risk of being wrong. Inherent to the concept of accuracy is that the analytic message a customer receives should be the one the analyst intended to send. Therefore, analytic products should express judgments as clearly and precisely as possible, reducing ambiguity by addressing the likelihood, timing, and nature of the outcome or development. Clarity of meaning permits assessment for accuracy when all necessary information is available.

(9) Incorporates effective visual information where appropriate: Analytic products should incorporate visual information to clarify an analytic message and to complement or enhance the presentation of data and analysis. In particular, visual presentations should be used when information or concepts (e.g., spatial or temporal relationships) can be conveyed better in graphic form (e.g., tables, flow charts, images) than in written text. Visual information may range from plain presentation of intelligence information to interactive displays for complex information and analytic concepts. All of the content in an analytic product may be presented visually. Visual information should always be clear and pertinent to the product's subject. Analytic content in visual information should also adhere to other analytic tradecraft standards.