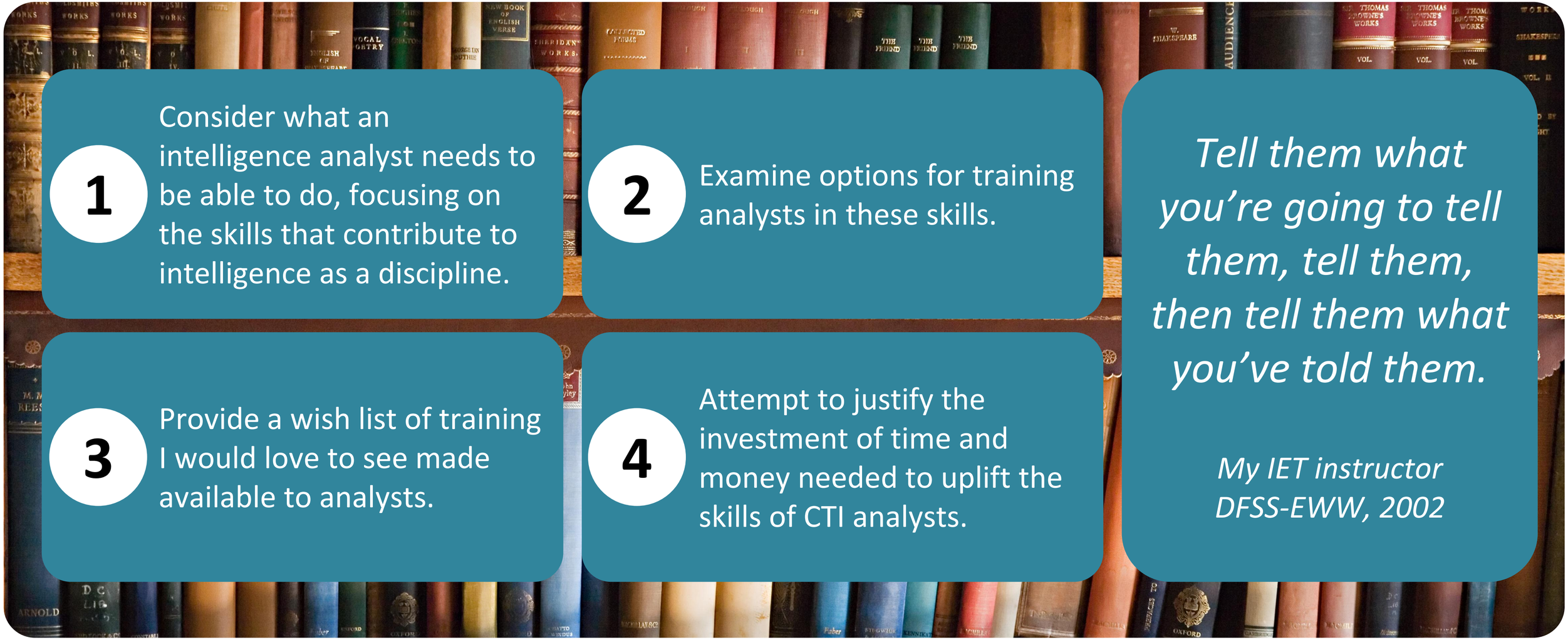
Teaching the intelligence bits of cyber threat intelligence

Brendon Hawkins

Today’s objectives



1. Consider what an intelligence analyst needs to be able to do, focusing on the skills that contribute to intelligence as a discipline.
2. Examine options for training analysts in these skills.
3. Provide a wish list of training I would love to see made available to analysts.
4. Attempt to justify the investment of time and money needed to uplift the skills of CTI analysts.

Tell them what you’re going to tell them, tell them, then tell them what you’ve told them.

My IET instructor
DFSS-EWW, 2002

Intelligence analysis at its most basic

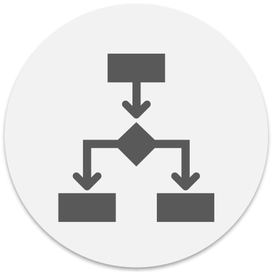
Intelligence analysts build an understanding of the enterprise…

…and use their knowledge about the threat landscape to go looking for relevant threats.

They find data, bring it into one place, and evaluate it…

…before they use their subject matter expertise to perform intelligence analysis.

The output of this analysis is used to produce intelligence…



…which is communicated to other parts of the enterprise…

…to support decision makers.

For today, I’d like you all to step back and think about Cyber Threat Intelligence (CTI) as an intelligence discipline where the threat actor is targeting an organisation through its IT infrastructure.

Intelligence Analysis: Does NSA Have What It Takes?

[redacted] (b)(3)-P.L. 86-36

INTRODUCTION

> Seekers of Wisdom first need sound intelligence. Heraclitus [1]

Do National Security Agency (NSA) intelligence analysts have what it takes to be successful? What is a successful analyst? Indeed, what is analysis?

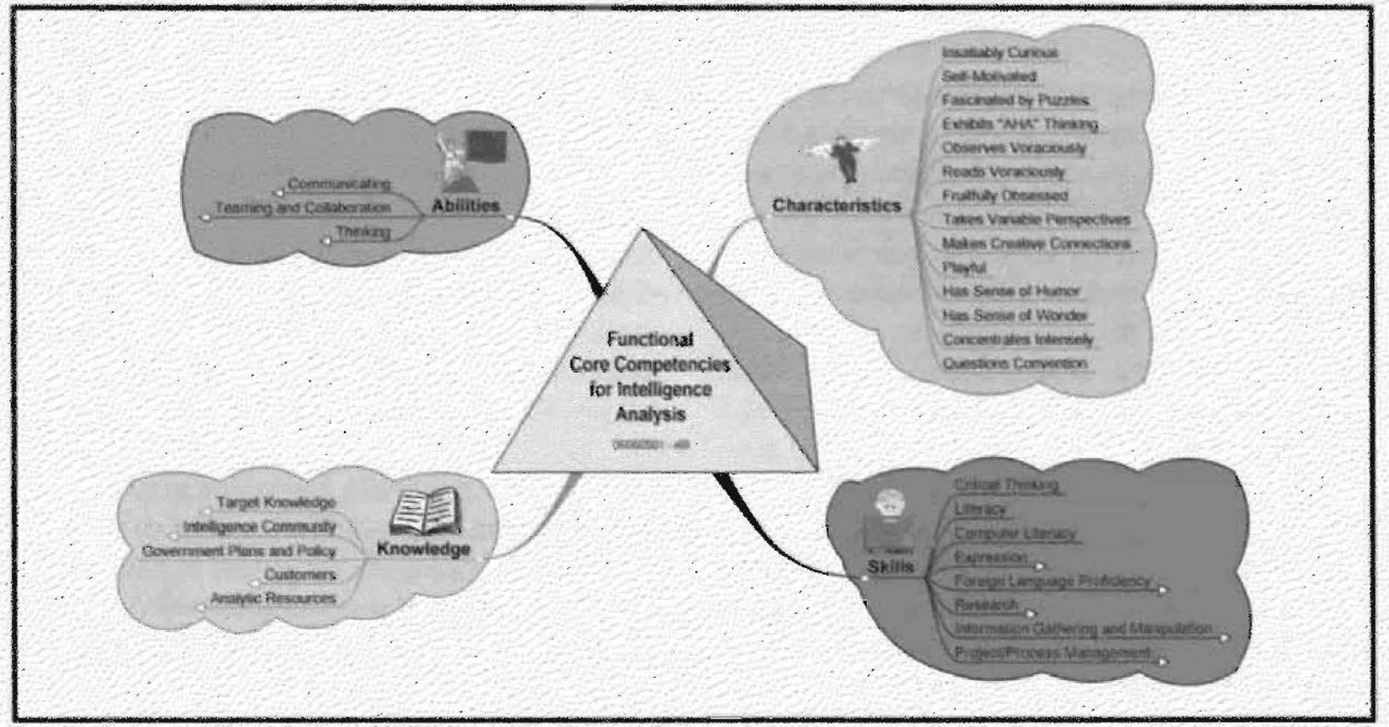
These questions strike at the heart of NSA's mission to provide intelligence to national leaders and decision makers. The imperative to answer these questions stems from two types of pressures, external and internal. Externally, NSA faces a changed world order that demands responsiveness, agility, and flexibility at a moment's notice in response to diverse transnational threats. Internally, NSA is charged with transforming outdated Cold War organizational structure, mentality, and methods to counter those challenges.

The 21st century is filled with complex, rapidly changing intelligence problems that challenge contemporary intelligence agencies to extend well beyond their traditional purview. Whereas in the 20th century the major threats to American security were considered monolithic, today diverse nonstate or antistate actors deliberately threaten the security of the United States in ways that extend far beyond the traditional political and military realms. Consequently, intelligence consumers need to know about the intentions and actions of what Adda Bozeman refers to as the "other" in her seminal work on strategic intelligence and statecraft.[2] Two examples of the significant threats posed by "others" are terrorism and transnational crime. Religious and ethnic terrorism increased through the 1990s and continues to increase in the first decade of the new century.[3] Former secretary of state Warren Christopher noted that increasing religious and ethnic terrorism has become "one of the most important security challenges we face in the wake of the Cold War."[4] Similarly, transnational criminal enterprises pose a significant threat. Insinuated into weak governments and nongovernmental institutions, they derive income from "alien smuggling; trafficking in women and children; smuggling toxic materials, hazardous wastes, illicit arms, military technologies, and other contraband; financial fraud; and racketeering."[5] Costing about one percent of global GNP, these enterprises threaten both the American way of life and its quality.[6]

To counter these, and myriad other 21st century threats, policymakers, decision makers, and military leaders require on-time, actionable intelligence. Thus President Bush's directive ordering a comprehensive review of U.S. intelligence begins "[current] and accurate foreign intelligence is essential to the success of our foreign policy, law enforcement, and defense strategies and is critical to protecting and advancing America's vital interests."[7] NSA, along with other agencies within the intelligence community, must adapt to provide that intelligence. To successfully do so requires a new paradigm for intelligence analysis and production.

One of the ways NSA has begun to adapt is by envisioning an organizational model that places all intelligence analysts under the purview of an analytic deployment service, from which individuals are assigned to specific production lines based on the capabilities of the former and the needs of the latter. However, for this model to

Fig. 1. Functional core competencies for intelligence analysis



AUSTRALIAN CYBER CONFERENCE 2024
AISA

NSA core competencies for intelligence analysis

Characteristics

Curious
Self-Motivated
Fascinated with Puzzles
Exhibits A-ha Thinking
Observant
Reads
Fruitfully Obsessed
Takes Variable Perspectives
Makes Creative Connections
Playful
Exhibits a Sense of Humour
Exhibits a Sense of Wonder
Concentrates Intensely
Questions Convention

Abilities

Communicating
Teaming and Collaborating
Thinking

Skills

Critical Thinking
Literacy
Computer Literacy
Expression
Foreign Language
Research
Information Gathering
Project Management

Knowledge

Target Knowledge
Intelligence Community
Government Plans & Policy
Customers
Analytic Resources

Rigorous Analysis

Holistic
Competitive
Adds Value
Highest Level Possible

Management

Customer Relations
Community Relations
Resource Allocation
Organization of Work
Empowering Analysis
Valuing Analysis

Meets /Anticipates Customer Needs

Readiness
Timeliness
Accuracy
Objectivity
Usability
Relevance

Conveys Intelligence

Analytic Conclusions
Decision Points
Implications of Choices

The point here is not to focus on the details of a 25-year-old think piece: it's that when they went through what they needed out of their intelligence analysts, most of it wasn't technical skills, even at NSA, the most technical intelligence agency.

Duties of a CTI analyst

Intelligence analysts of all disciplines are required to have a broad variety of skills as well as at least one area of deep subject matter expertise.

An ideal cyber threat intelligence analyst:

- Writes at a postgraduate level.
- Has elite technical skills.
- Is comfortable engaging with leadership.
- Can knock up a briefing in 5 minutes.
- Is able focus deeply on complex analytic tasks.
- Can seamlessly multitask.
- Is able to code and automate workflows.

Often a corporate intelligence capability is a single individual who needs to do it all.

Mapping CTI against the intelligence cycle

Intelligence is often just thought of as a product.

But what separates intelligence from other types of information or knowledge is that it has been through a **process** of selection, processing, evaluation, synthesis, analysis, and communication.

The intelligence analyst is the master of this process. The question is how do we teach these skills.

Planning and Direction

Gathering requirements
Eliciting feedback
Stakeholder engagement
Metrics
Project management

Collection

Collection planning
Collection management
Onboarding new sources
OSINT
Writing and tuning rules

Processing

Managing platforms
Knowledge bases
Automating feeds
Triaging raw intelligence
Evaluating intelligence

Analysis and Production

Data and log analysis
Writing reports
Information synthesis
Reading, reading, reading
Producing data products

Dissemination

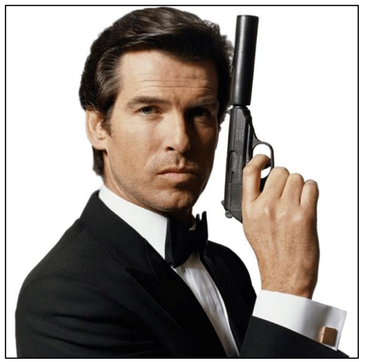
Engaging with leadership
Briefing intelligence
Managing communities
Establishing and maintaining comms channels

Where do we learn CTI skills?

Cyber Skills

Most CTI analysts will have a strong technical background (Cyber, IT or Computer Science) from tertiary education. Many will have experience in other cyber roles.

Intelligence Skills



Military and intelligence agencies

Public and private courses

On-the-job training

Option 1: recruit from government

- Government intelligence analysts will have been trained in intelligence as a discipline.
- They may have existing target or technical knowledge.
- Often they have worked a range of targets making them adaptable

- They may still require further technical training.
- They may not have a solid background in broader corporate cyber operations.
- Government analysts will need to adapt to a corporate culture.
- Must adjust to a different mission.

In a larger CTI team, having a mix of intelligence analysts from both a technical cyber background and a government intelligence background is ideal. However, few corporate CTI teams operate at a scale where they have more than one or two analysts.

Option 2: training courses

- Universities offer degrees in intelligence.
- These courses focus on the core competences required to manage an intelligence capability.

- There are a range of private providers who offer CTI training.
- Some of these courses include modules for skills like critical thinking, recognising, bias etc.

- These post graduate courses start at 1 year of part time study.
- They are expensive.
- They are more suited to analysts moving into management.
- Focussed on theory over practical skills.

- They can be very expensive.
- There is generally a focus on cyber skills rather than broader intelligence skills.
- The one intelligence course in the VET training framework is not fit for purpose for CTI.

Charles Sturt University
Master of Intelligence Analysis

Essential set - Core subjects

JST450	Introduction to Intelligence	8 credit pts
JST428	Operational Intelligence	8 credit pts
JST495	Intelligence and Analytics	8 credit pts
JST452	Intelligence Management	8 credit pts
JST541	National Security and Intelligence	8 credit pts
JST555	Open Source Intelligence (OSINT)	8 credit pts

Macquarie University
Master of Intelligence

Core Zone — **80 credit points**

Essential units — **60 credit points** — Complete each unit below.

PICT8012 Critical Thought and Research Design	10
PICT8013 History of Intelligence	10
PICT8014 Intelligence Ethics and Oversight	10
PICT8003 Emerging Topics in Security Studies	10
PICT8044 Intelligence Analysis	10
PICT8045 Intelligence: Theory and Practice	10

DEF40217 - Certificate IV in Intelligence Operations

Code	Status
DEFINT002- Plan and lead a counter-surveillance operation	Core
DEFGEN007- Conduct risk assessment in a Defence environment	Core
PUACOM007B- Liaise with other organisations	Core
DEFINT001- Supervise intelligence operations	Core
PSPGEN027- Gather and analyse information	Core
BSBWRT401- Write complex documents	Core
BSBTEC402- Design and produce complex spreadsheets	Elective
PSPSEC007- Develop and advise on government security procedures	Elective
DEFGEN003- Lead a team	Elective
BSBPMG424- Apply project human resources management approaches	Elective
BSBWHS311- Assist with maintaining workplace safety	Elective
PSPGEN130- Use resources to achieve work unit goals	Elective
DEFGEN012- Provide technical advice	Elective
BSBPMG425- Apply project information management and communications techniques	Elective
BSBMKG555- Write persuasive copy	Elective
BSBPMG430- Undertake project work	Elective

Code	Status
PSPINV001- Plan and initiate an investigation	Elective
PSPSEC022- Implement security risk treatments	Elective
PSPINV004- Conduct an investigation	Elective
BSBPMG420- Apply project scope management techniques	Elective
BSBITU402- Develop and use complex spreadsheets	Elective
PSPSEC012- Develop security risk management plans	Elective
DEFINT003- Edit intelligence material for security purposes	Elective
BSBWHS411- Implement and monitor WHS policies, procedures and programs	Elective
PSPINV003- Finalise an investigation	Elective
BSBPMG428- Apply project life cycle management processes	Elective
DEFGEN010- Supervise equity and diversity in the workplace	Elective
BSBCMM411- Make presentations	Elective
PSPGEN138- Organise workplace information	Elective
PUATEA002- Work autonomously	Elective
PSPINV001- Plan and initiate an investigation	Elective

Qualification Description

This qualification allows for the attainment of competencies in Defence intelligence operations including personnel working in operational roles and undertaking and leading intelligence operations in a Defence or similar government environment.

Option 3: on-the-job training

- Training can be tailored to the capabilities of the analysts in the team.
- Training can be delivered at a convenient time and pace.
- Training can be aligned with uplift and work activities in the team.

- Someone needs to develop and deliver the training.
- Generally, this falls to a senior member of the team, who may not have the time to spare.
- It requires an intelligence function at the scale where developing training in-house is worthwhile.

Even senior analysts within CTI may not necessarily have the breadth of intelligence exposure to teach the general intelligence skills and processes, because most CTI capabilities don't operate on the scale of government intelligence agencies.

On-the-job training at ANZ

When examining what was needed for intelligence training within the CTI team at ANZ, it was recognised that the team had exceptional technical skills but had not been exposed to broader intelligence practices.

1. What is intelligence?
2. The Intelligence Cycle
3. Intelligence Requirements
4. Admiralty Code and Words of Estimative Probability
5. Data, Information, Knowledge and Wisdom
6. Collection Management
7. Who What Where When How Why and Whither
8. Information Reports
9. Writing Intelligence Reports
10. Processing Intelligence using AI

These ten modules were delivered over the course of a year, one per month, and were generally very well received. However, there is a need for more training, and it was a challenge to continually develop and deliver training while managing a team. Ultimately, it’s unsustainable.

What I’d like for intelligence analyst training

Introduction to intelligence
- What is intelligence
- Types of intelligence
- Professions in intelligence

Introduction to the Intelligence Cycle
- Intelligence as a process
- Planning and direction (requirements)
- Collection
- Processing
- Analysis and production
- Dissemination
- Feedback and Evaluation

Conceptual foundations of intelligence analysis
- Bias & Logic
- Intelligence failures
- Data, information, knowledge and wisdom
- WWWWHW&W
- Introduction to ontology

The target
- Target discovery
- Target development
- Turning intelligence into target knowledge
- Empathy – understanding your target’s perspective
- Cultural considerations

Ethics and intelligence
- Privacy
- Proportionality
- Legal compliance
- Managing sensitive data

Collection management
- Collection management matrix
- Collection operations planning
- Collection operations management
- Managing OSINT activities
- Onboarding collection sources
- Collection metrics

Processing intelligence
- Evaluating source reliability
- Evaluation information quality
- Structuring unstructured information
- Developing intelligence ontologies
- Processing intelligences using AI

Analytic technique
- Induction and deduction
- Analysis using DIKW
- Aggregating data using basic statistical methods
- Temporal analysis
- Network analysis
- Geospatial analysis
- Progressing from platform to tool to scripts
- Structured analytic techniques
- Applying data science and AI for intelligence analysis
- Python for intelligence analysis

Report writing
- Using words of estimative probability
- Analyst comments and assessments
- Information reports
- Intelligence reports
- Intelligences assessments

Dissemination
- Briefing intelligence
- Understanding your audience
- Tailored intelligence reporting

Managing Intelligence
- Stakeholder engagement
- Requirements and feedback
- Managing intelligence analysts
- How to say no to senior managers
- Applying metrics to an intelligence capability
- Full-cycle intelligence management

Some practical considerations

That’s a lot of training!

Yes, but it can take a decade or more to build a senior intelligence analyst.

Who could deliver this?

Government?
Private enterprise?
Loose coalition of desperate intelligence managers?

Is there demand?

This is a lot of the reason why I put this presentation together:

Do analysts feel they need this type of training?

Why do I think there is a need?

1. CTI in corporate cyber security functions has rapidly changed from simply ingesting and matching IOC strings to complex analysis done in-house, narrative intelligence reporting, long-term assessments, and advising senior executives on strategy and procurement.

2. Intelligence functions within companies therefore require more active management grounded in a comprehensive understanding of how intelligence works.

3. The skills and experience to manage a full intelligence capability are rare in a single individual. Even intelligence agencies rely on hundreds of specialised staff each fulfilling a small part of the intelligence cycle.

4. Corporate CTI teams will necessarily operate at a small scale. While vendors can assist (and some are truly excellent), the CTI team must manage the full capability and contextualise intelligence to the organisation’s requirements.

CTI analysts trained in broad intelligence practices will better meet the needs of their organisation

Conclusion

We've gone through the skills that intelligence analysts need

We've examined existing training options

We've considered what a curriculum could look like

I've had a go at trying to convince you why it's needed

Any questions or comments?

Thank you!

Brendon Hawkins