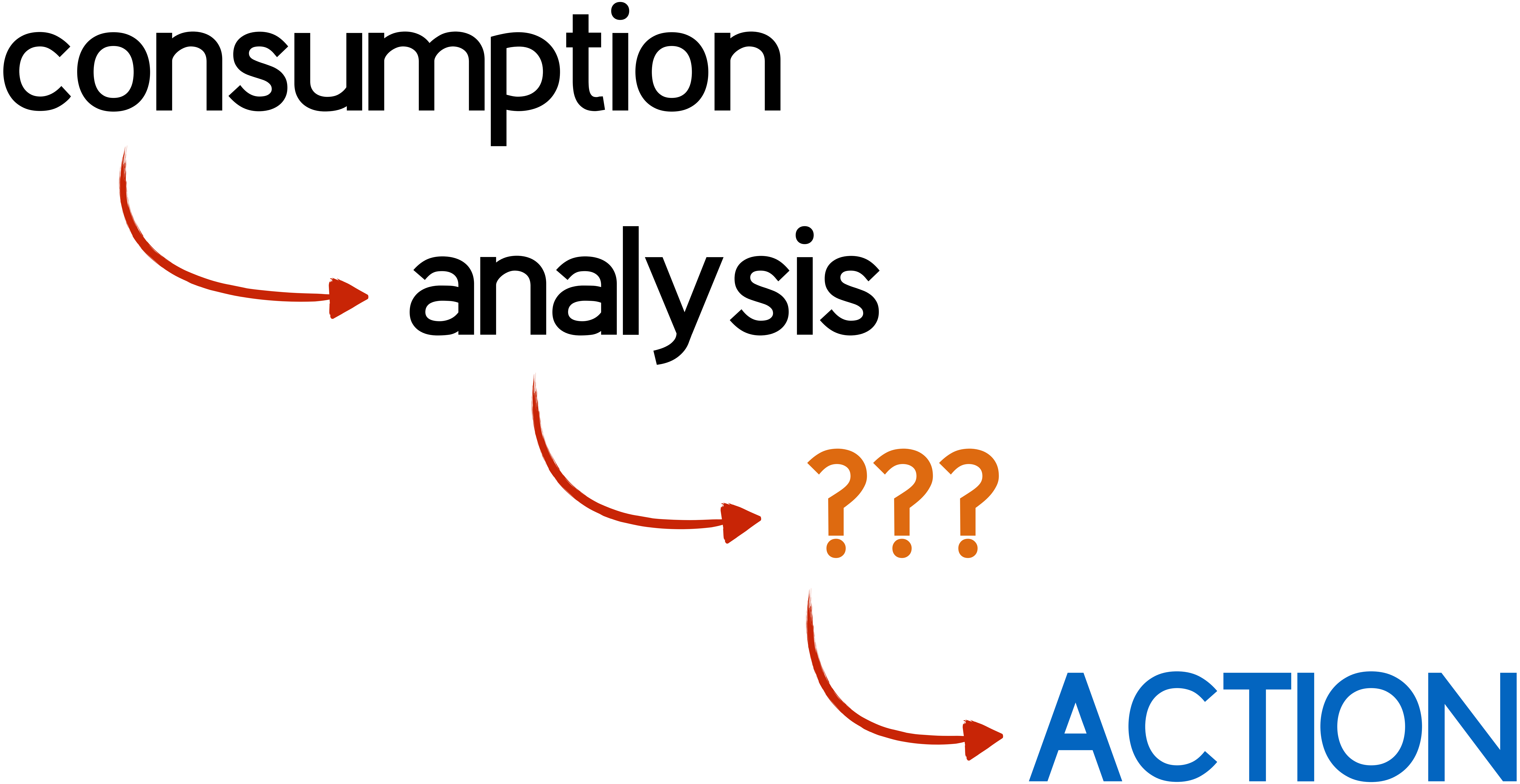
Pen-to-Paper & the Finished Report

The (Often Overlooked) Key to Generating Threat Intelligence

Who am I?

Christian Paredes (@cyint_dude)

- Booz Allen Hamilton since ~2010
- threat intel @ BAH since ~2012
- threat intel analysis & program build



consumption

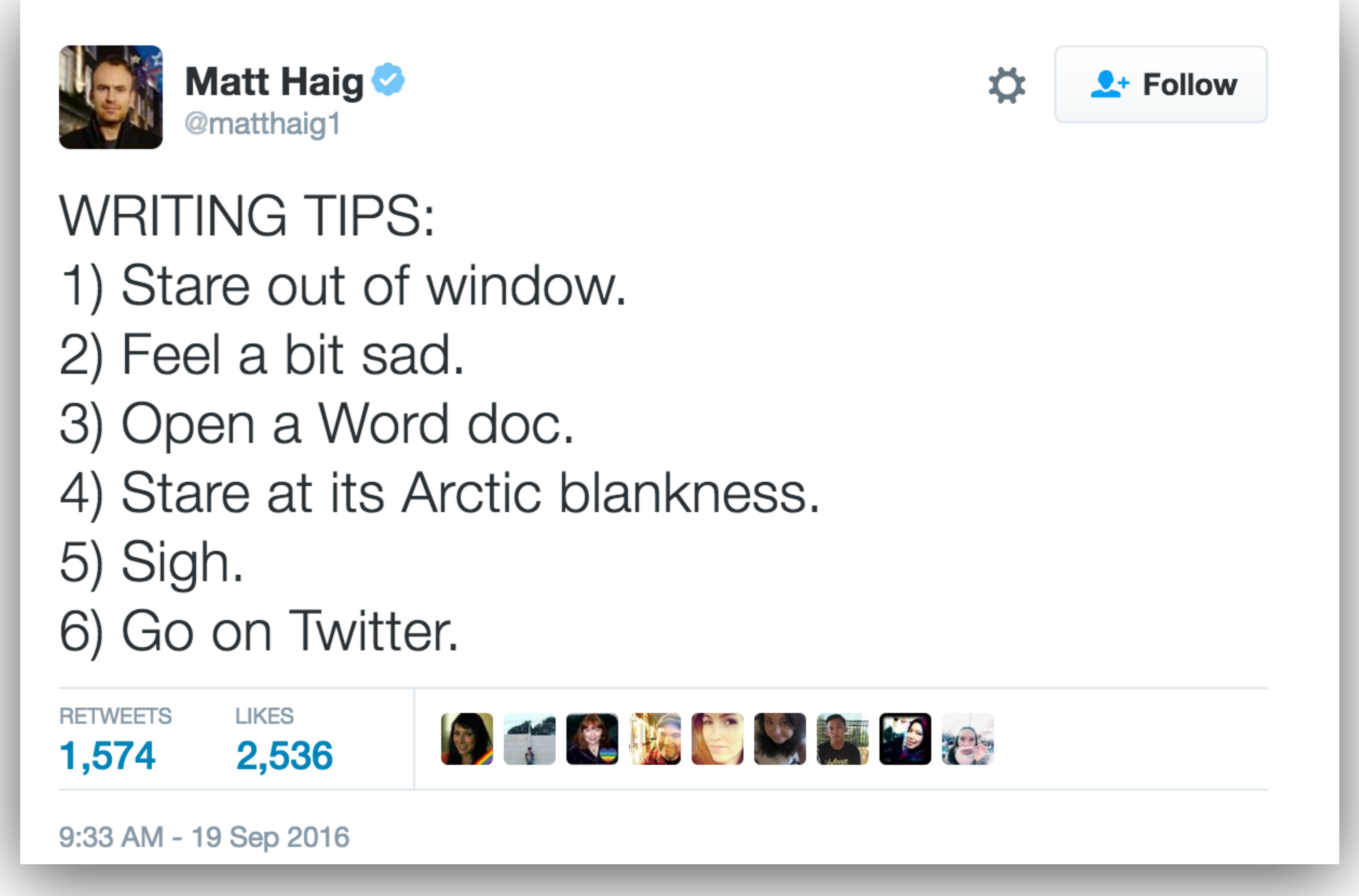
analysis

???

ACTION

finished reporting is the *only* way to:

* memorialize analysis; make it transparent and accessible
* preserve knowledge
* create accountability



Matt Haig
@matthaig1

WRITING TIPS:
1) Stare out of window.
2) Feel a bit sad.
3) Open a Word doc.
4) Stare at its Arctic blankness.
5) Sigh.
6) Go on Twitter.

RETWEETS 1,574
LIKES 2,536

9:33 AM - 19 Sep 2016

Process faults

Cognitive limitations

Complexity of threats

Source: Icons made by Anatoly from www.flaticon.com

A funny contradiction...

What we say

IOC != Intelligence!

Context is king!

Source: Icons made by Anatoly from www.flaticon.com

A funny contradiction…

What we say

and…

What we do

IOC != Intelligence!

Context is king!

1. Investigate!
2. Lots of notes, IOC
3. ~ fin ~

Source: Icons made by Anatoly from www.flaticon.com

"The capacity of working memory is tiny: it can only deal with about seven items of information at once."

~

Richard S. Sinclair, "Thinking and Writing: Cognitive Science and Intelligence Analysis," Center for The Study of Intelligence, Central Intelligence Agency, 1984

Source: Icons made by Anatoly from www.flaticon.com

Complex threats* → Tough questions

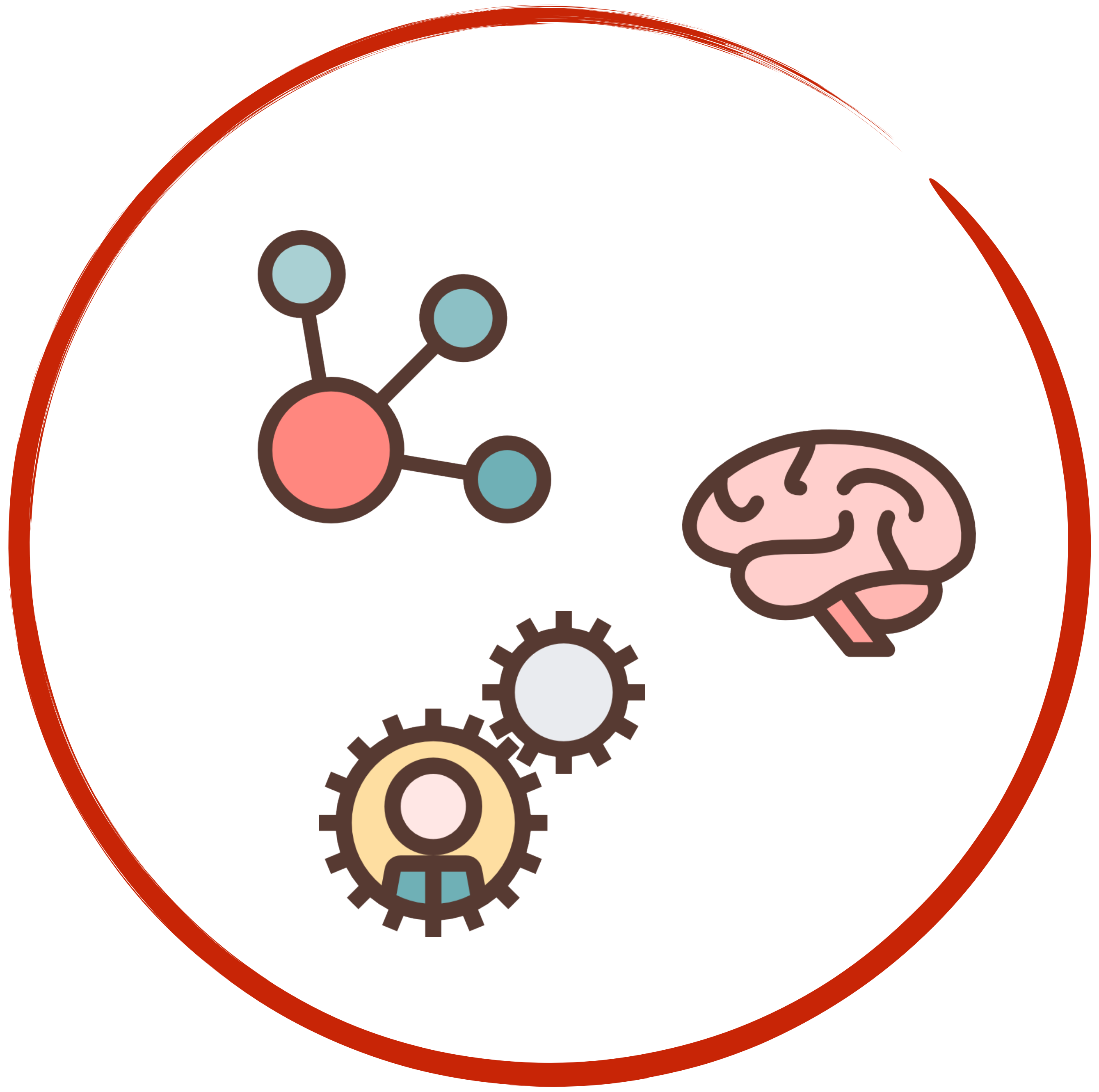
- Bangladesh Bank SWIFT heist
- DNC hack
- GRIZZLY STEPPE

- What happened?
- Are we at risk?
- Can we detect or prevent this threat?

* ugh, 2016.

Source: Icons made by Anatoly from www.flaticon.com

challenges result in...



- “analytic fragments”
- undocumented analysis
- unshared knowledge
- lack of continuity

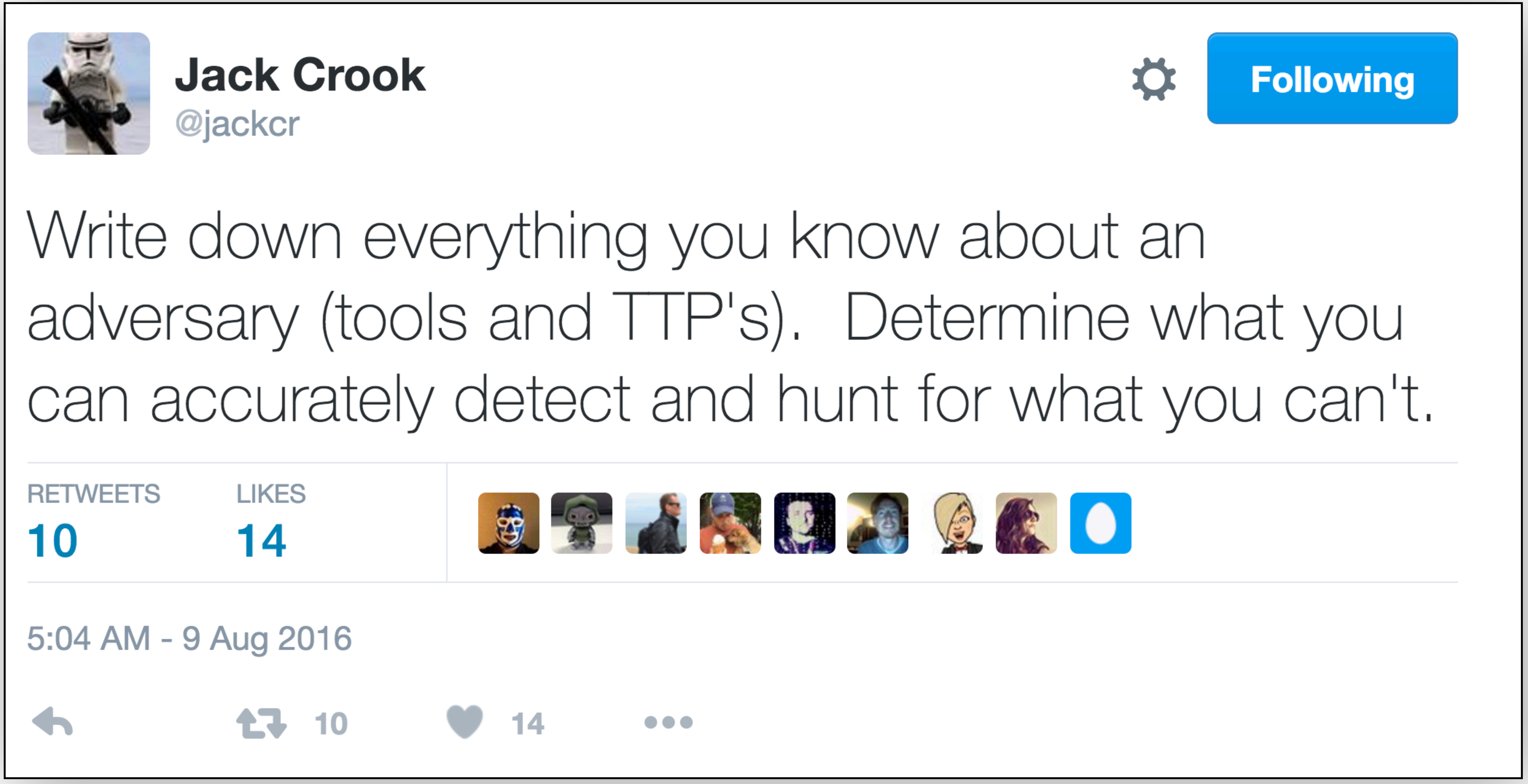
Source: Icons made by Anatoly from www.flaticon.com

"If we did nothing but marvel at the achievements of our minds we would leave a lot left unsaid."

~

Richard S. Sinclair, "Thinking and Writing: Cognitive Science and Intelligence Analysis," Center for The Study of Intelligence, Central Intelligence Agency, 1984

the finished report

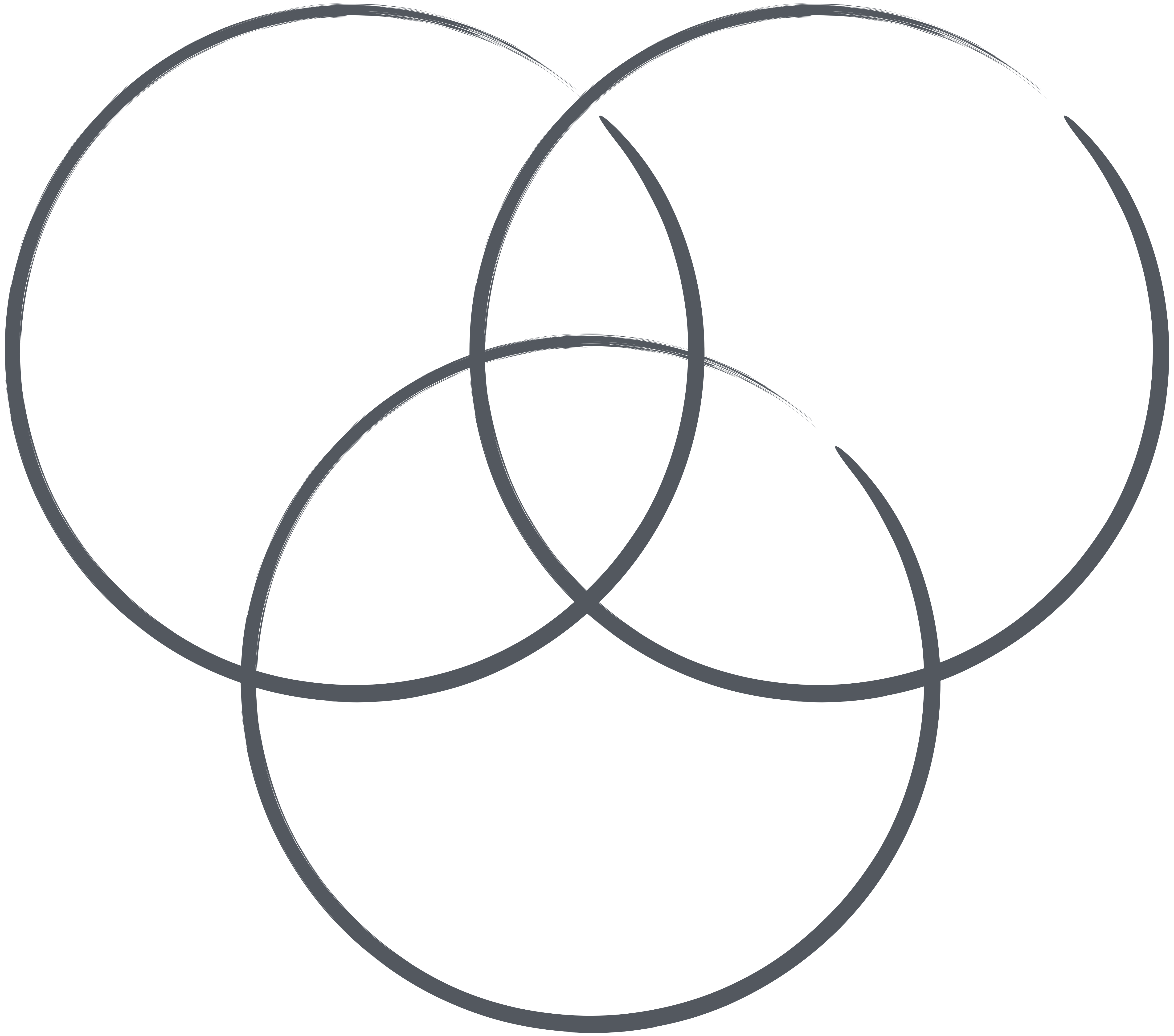


Jack Crook
@jackcr

Write down everything you know about an adversary (tools and TTP's). Determine what you can accurately detect and hunt for what you can't.

RETWEETS 10
LIKES 14

5:04 AM - 9 Aug 2016



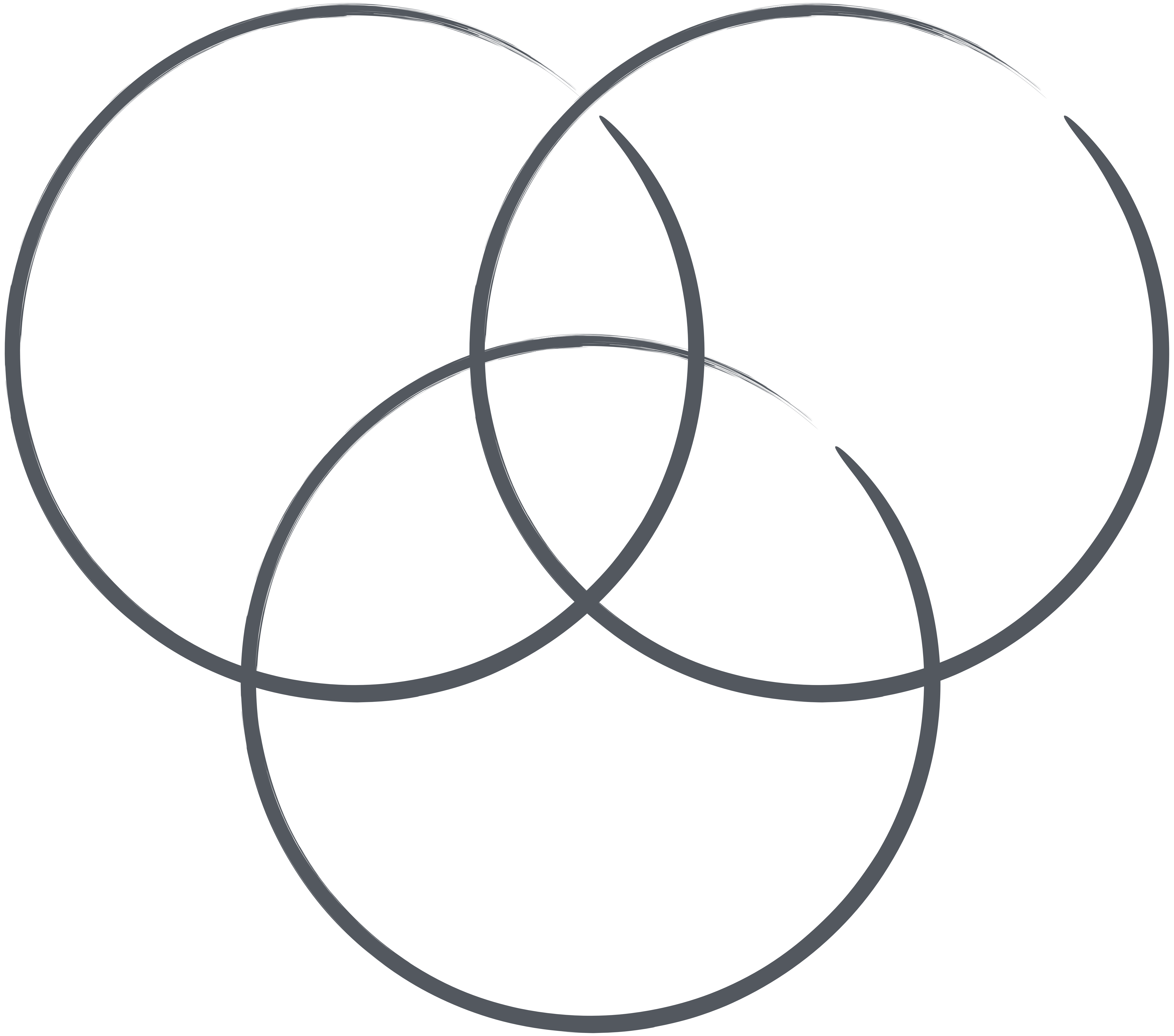
Structure

Style

So what?

Structure

- Title
- Summary & key points
- Logical flow

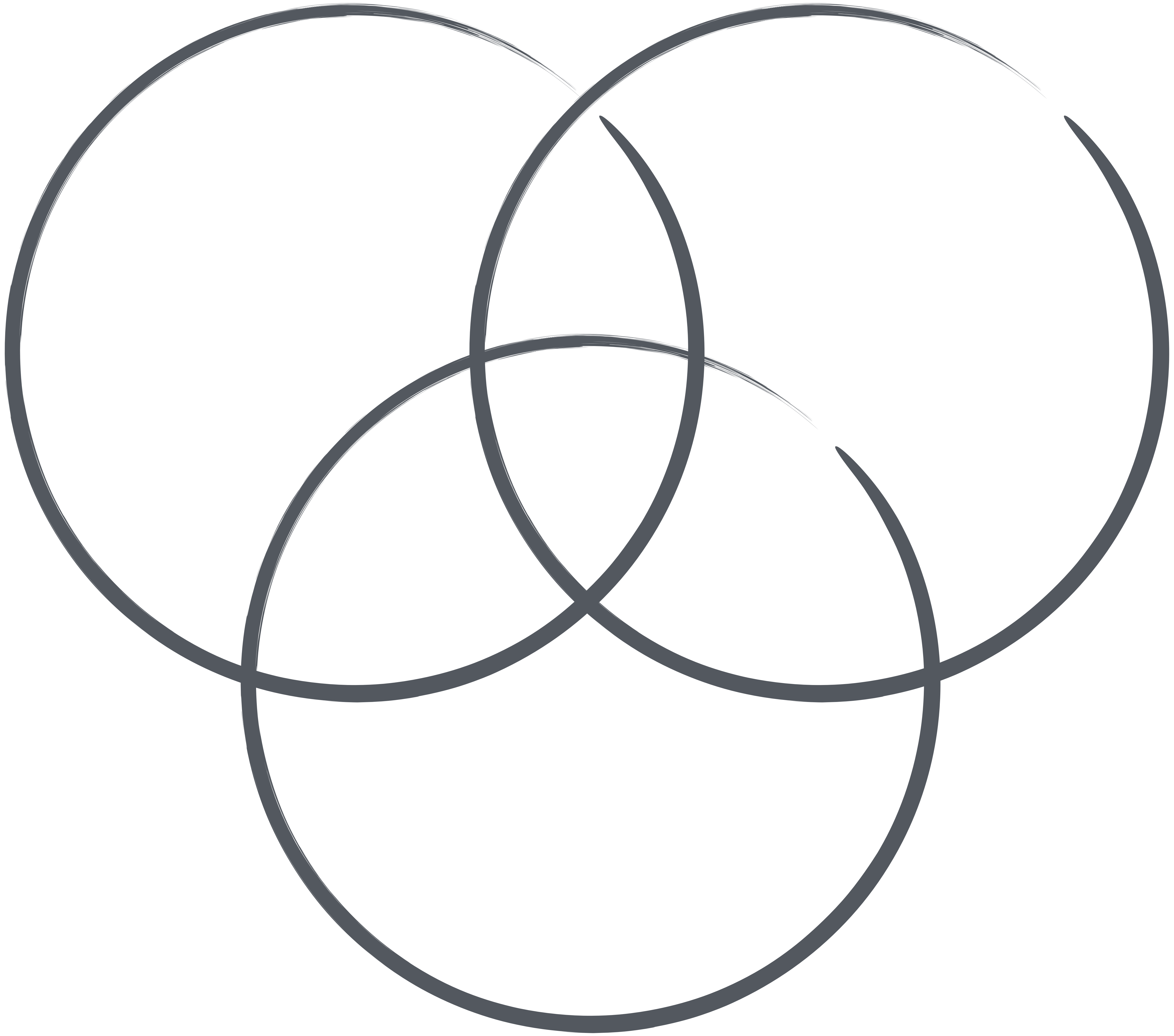


Style

So what?

Structure

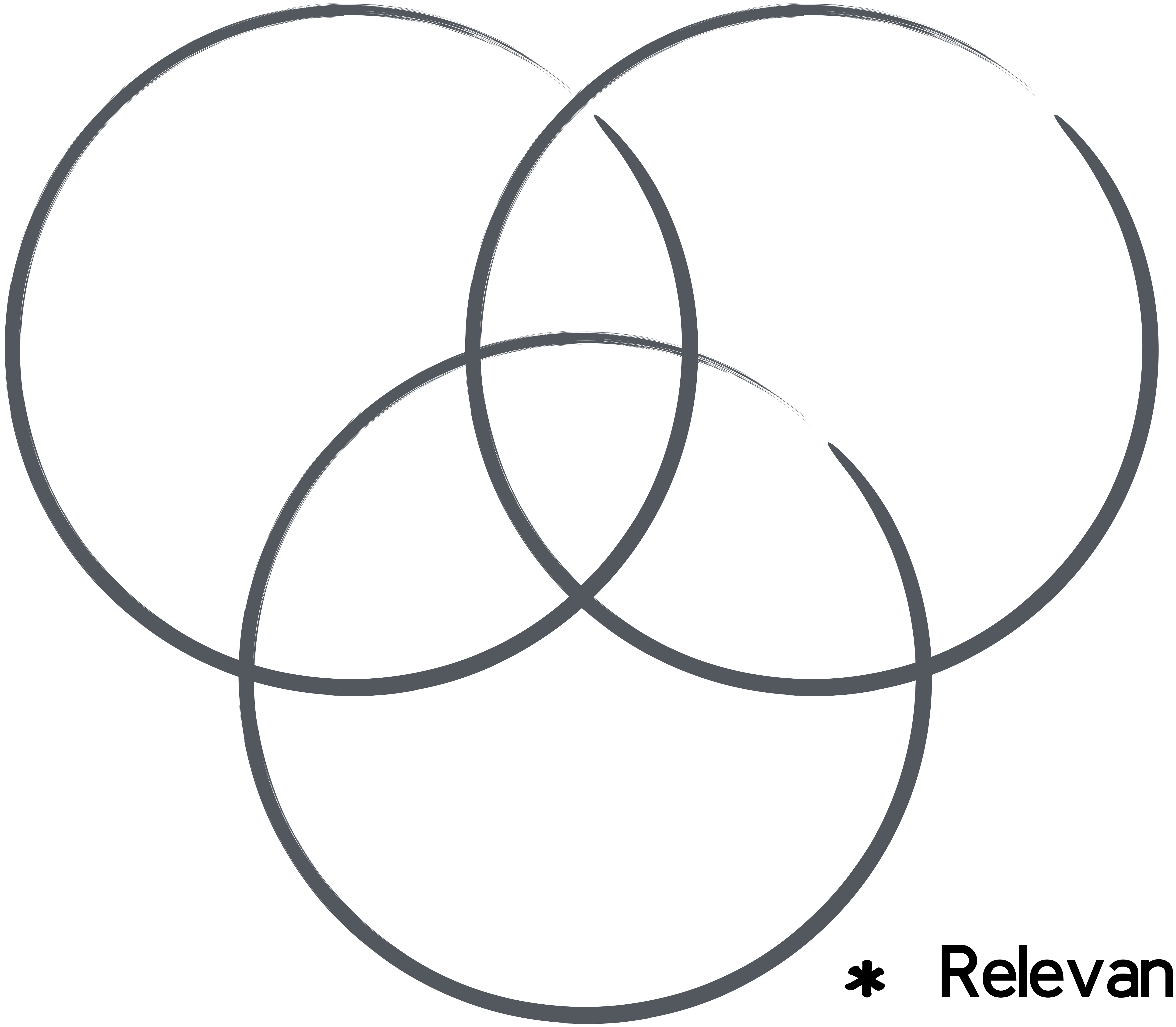
- Title
- Summary & key points
- Logical flow



Style

- Complete sentences
- Tailored to audience
- Conversational prose

So what?



Structure

- Title
- Summary & key points
- Logical flow

Style

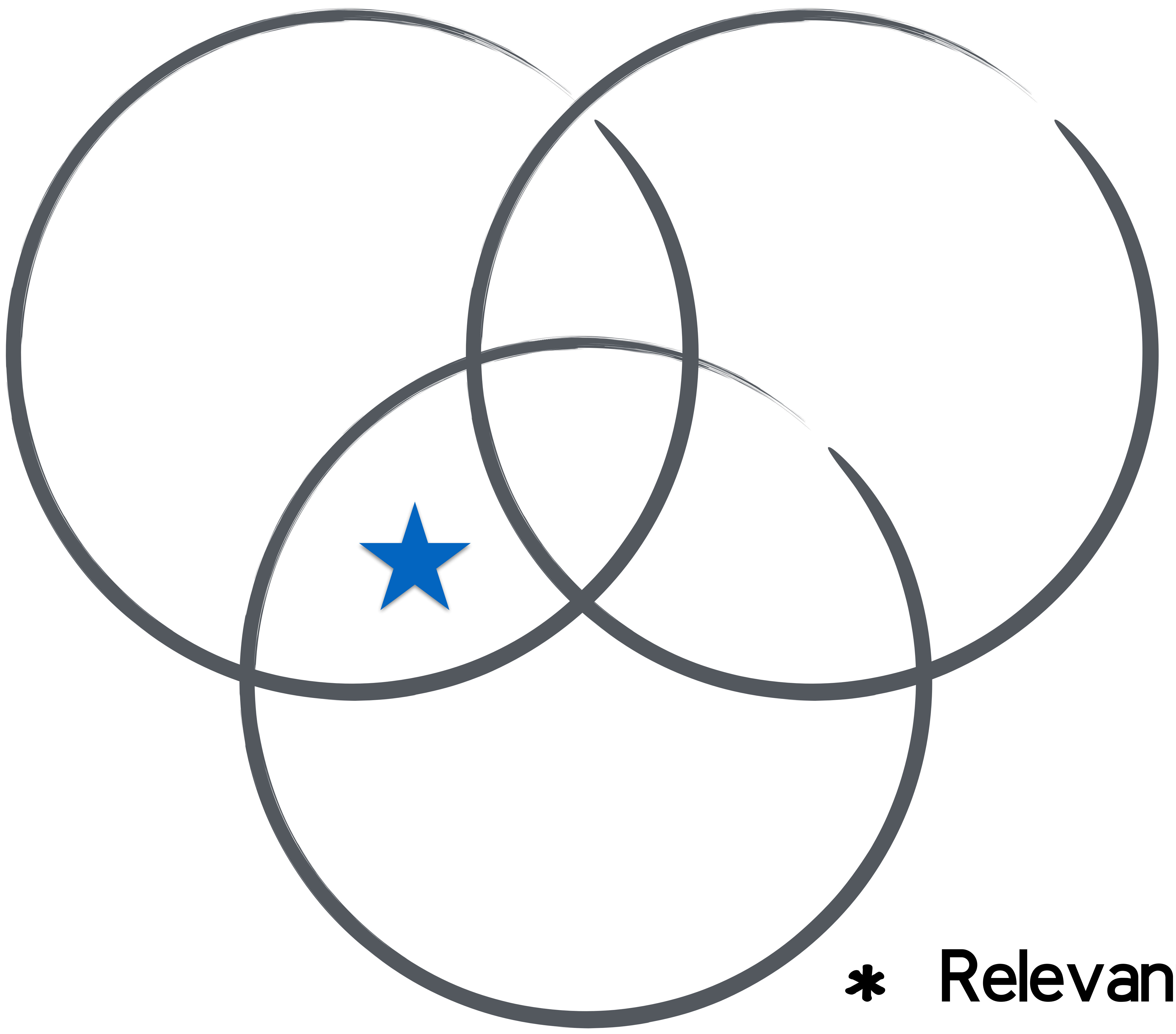
- Complete sentences
- Tailored to audience
- Conversational prose

So what?

- Relevant!
- Opportunities for the organization

Structure

- Title
- Summary & key points
- Logical flow

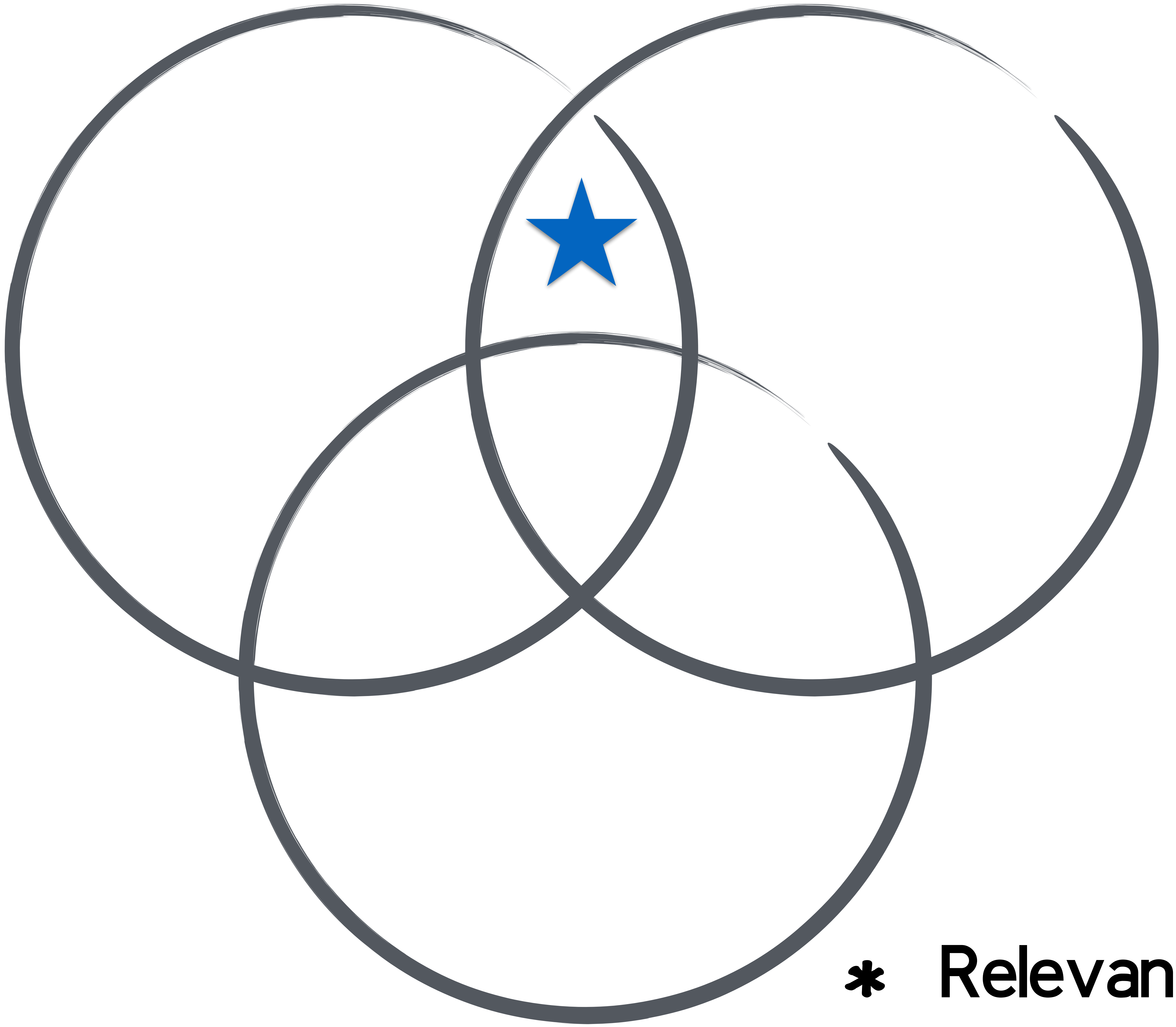


Style

- Complete sentences
- Tailored to audience
- Conversational prose

So what?

- Relevant!
- Opportunities for the organization



Structure

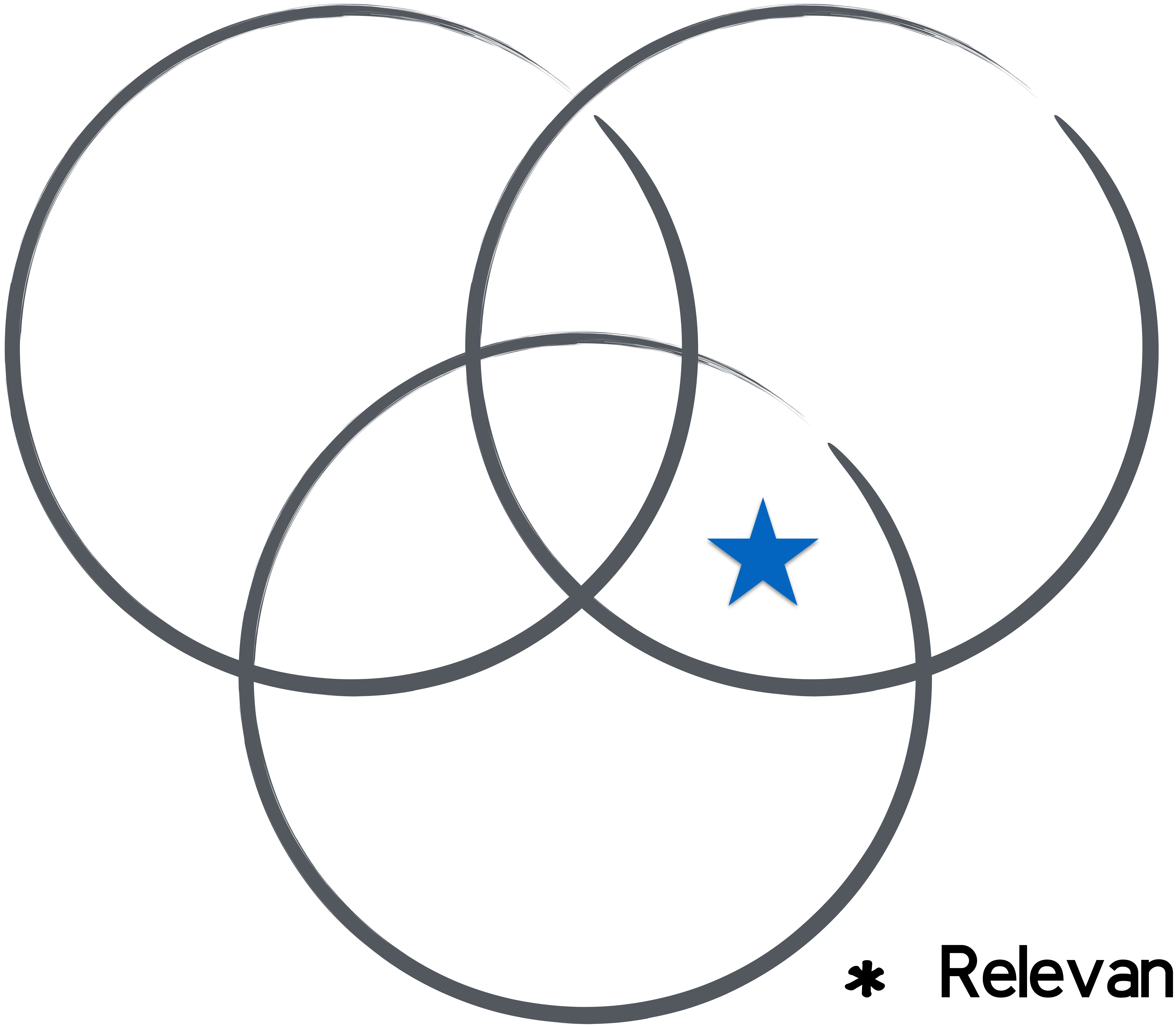
- Title
- Summary & key points
- Logical flow

Style

- Complete sentences
- Tailored to audience
- Conversational prose

So what?

- Relevant!
- Opportunities for the organization



Structure

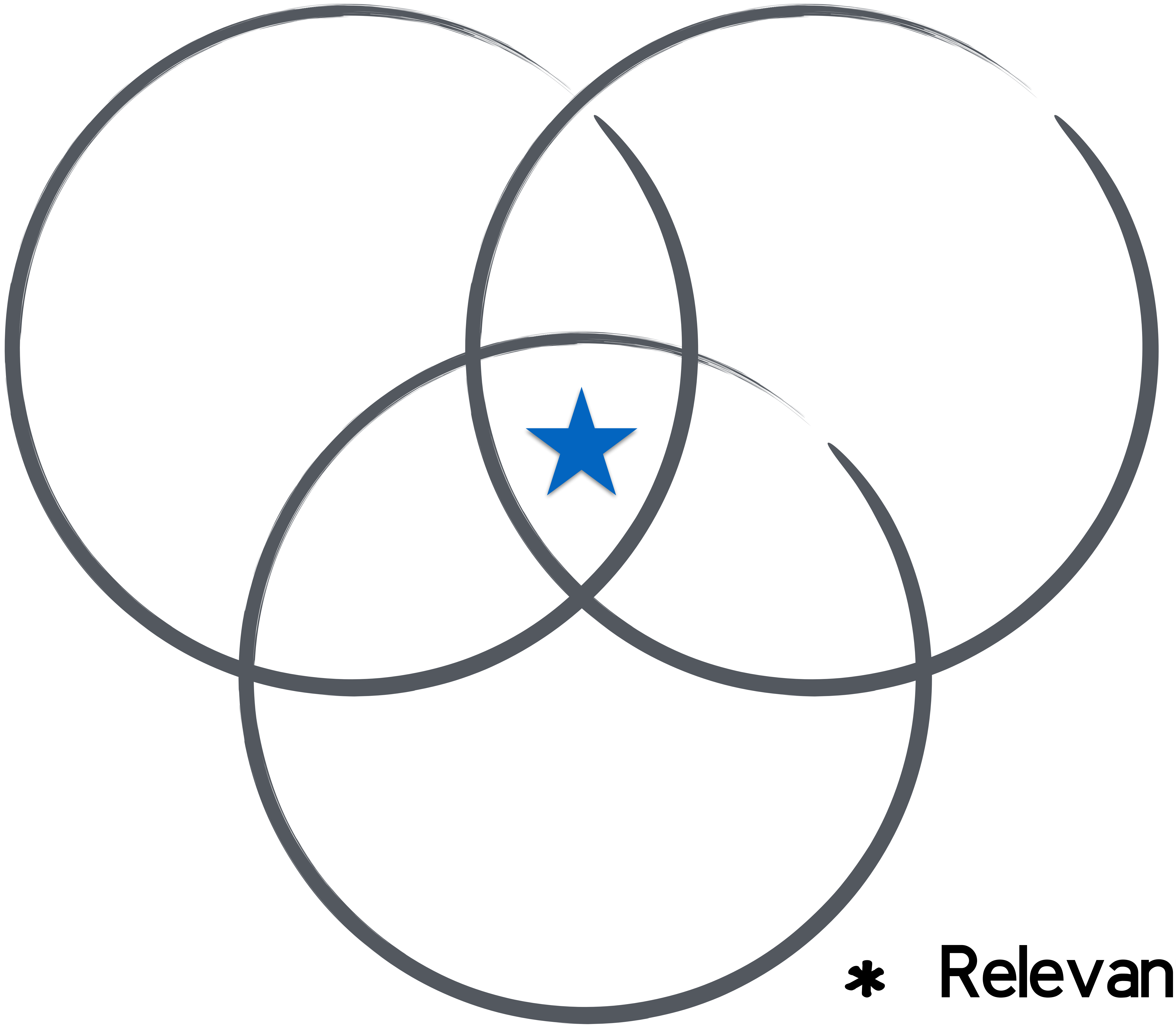
- Title
- Summary & key points
- Logical flow

Style

- Complete sentences
- Tailored to audience
- Conversational prose

So what?

- Relevant!
- Opportunities for the organization



Structure

- Title
- Summary & key points
- Logical flow

Style

- Complete sentences
- Tailored to audience
- Conversational prose

So what?

- Relevant!
- Opportunities for the organization

generating the finished report

TI Program { Institutionalize writing as critical tradecraft

TI Analyst { Hone writing skills

TI Program { Institutionalize writing as critical tradecraft

TI Analyst { Hone writing skills

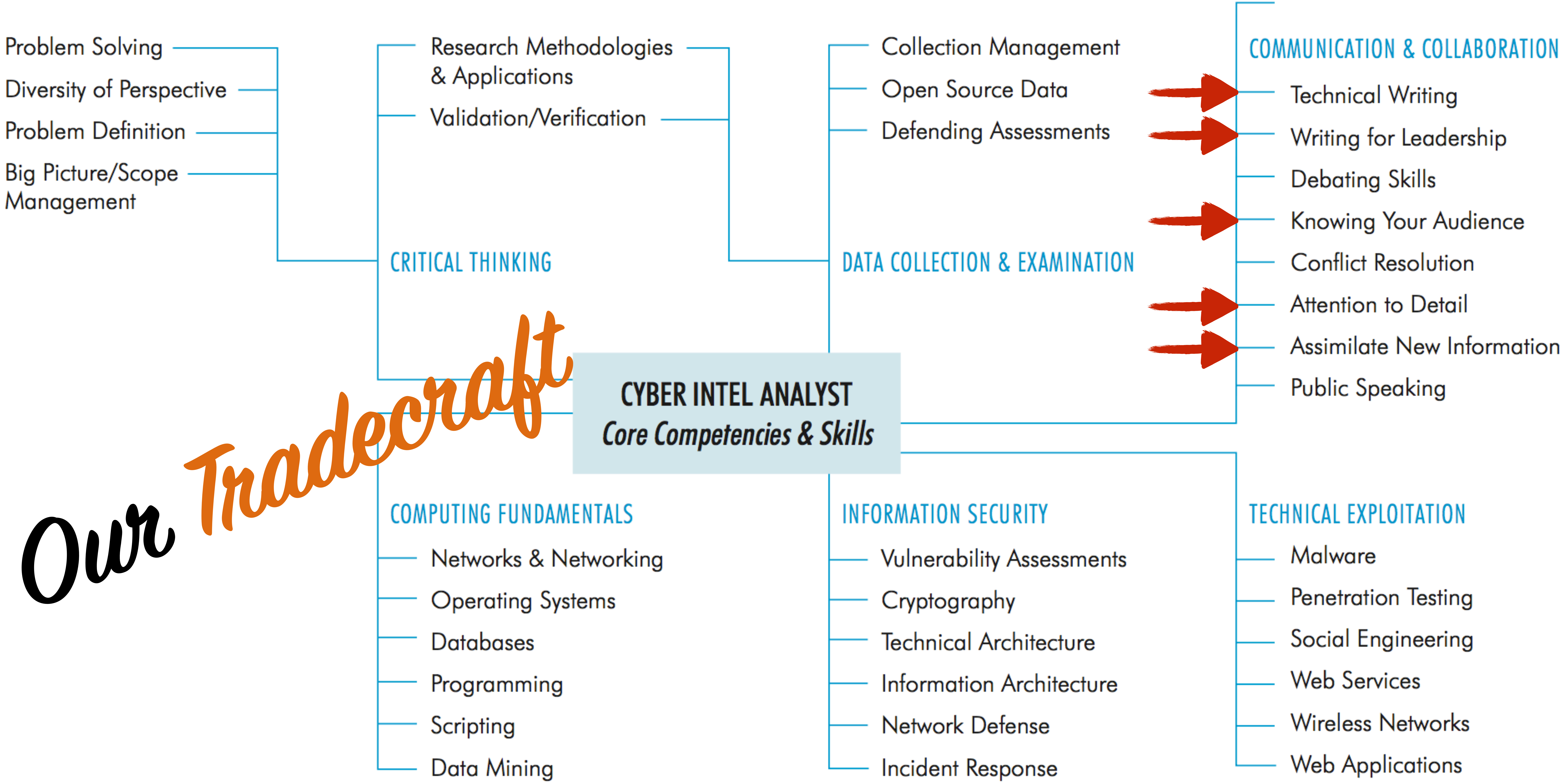
~ tradecraft ~

What is it?

АТЛАС
МОСКВА
с каждым домом
Такси Ми
Pepper Shield
586
500
RFID Shield

Hmm...

Our Tradecraft



CYBER INTEL ANALYST
Core Competencies & Skills

CRITICAL THINKING

- Problem Solving
- Diversity of Perspective
- Problem Definition
- Big Picture/Scope Management
- Research Methodologies & Applications
- Validation/Verification

DATA COLLECTION & EXAMINATION

- Collection Management
- Open Source Data
- Defending Assessments

COMMUNICATION & COLLABORATION

- Technical Writing
- Writing for Leadership
- Debating Skills
- Knowing Your Audience
- Conflict Resolution
- Attention to Detail
- Assimilate New Information
- Public Speaking

COMPUTING FUNDAMENTALS

- Networks & Networking
- Operating Systems
- Databases
- Programming
- Scripting
- Data Mining

INFORMATION SECURITY

- Vulnerability Assessments
- Cryptography
- Technical Architecture
- Information Architecture
- Network Defense
- Incident Response

TECHNICAL EXPLOITATION

- Malware
- Penetration Testing
- Social Engineering
- Web Services
- Wireless Networks
- Web Applications

Source: Cyber Intelligence: Preparing Today's Talent For Tomorrow's Threats," INSA, September 2015.

"Good intelligence depends in large measure on clear, concise writing...The information CIA gathers and the analysis it produces mean little if we cannot convey them effectively."

~

Style Manual and Writers Guide for Intelligence Publications, Central Intelligence Agency

TI Program { Institutionalize writing as critical tradecraft

TI Analyst { Hone writing skills

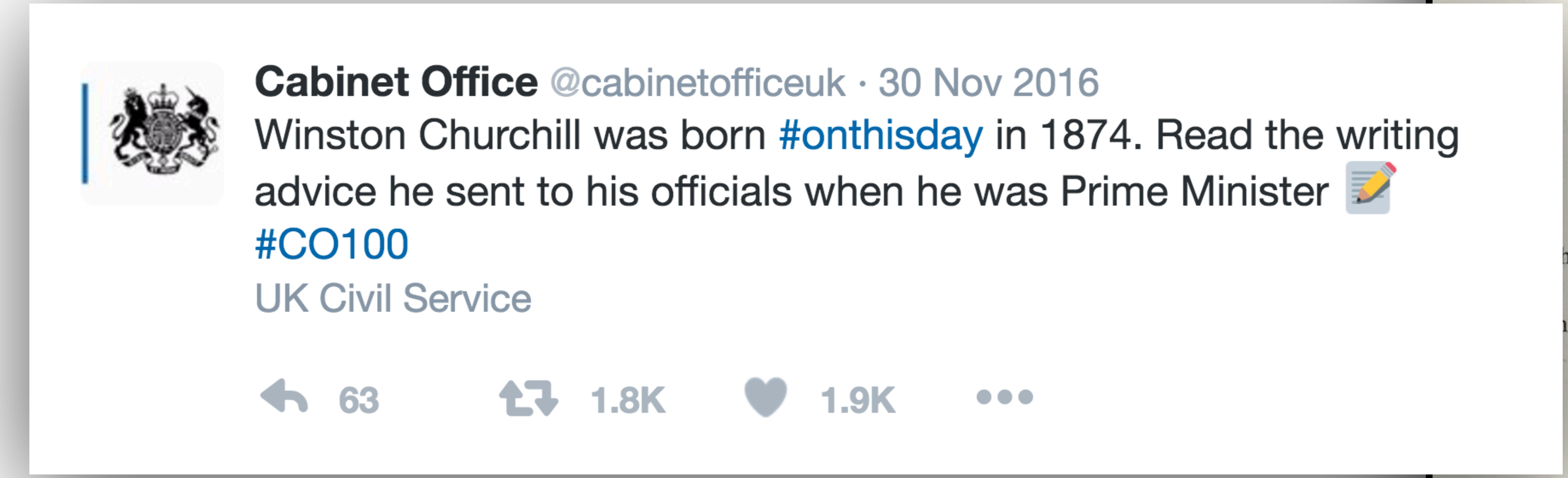
Really old school…

"Reading maketh a full man; conference a ready man; and writing an exact man…If a man write little, he had need have a great memory…."

Francis Bacon, "On Studies," early 1600s

Source: image from University of Cambridge.

Old school...

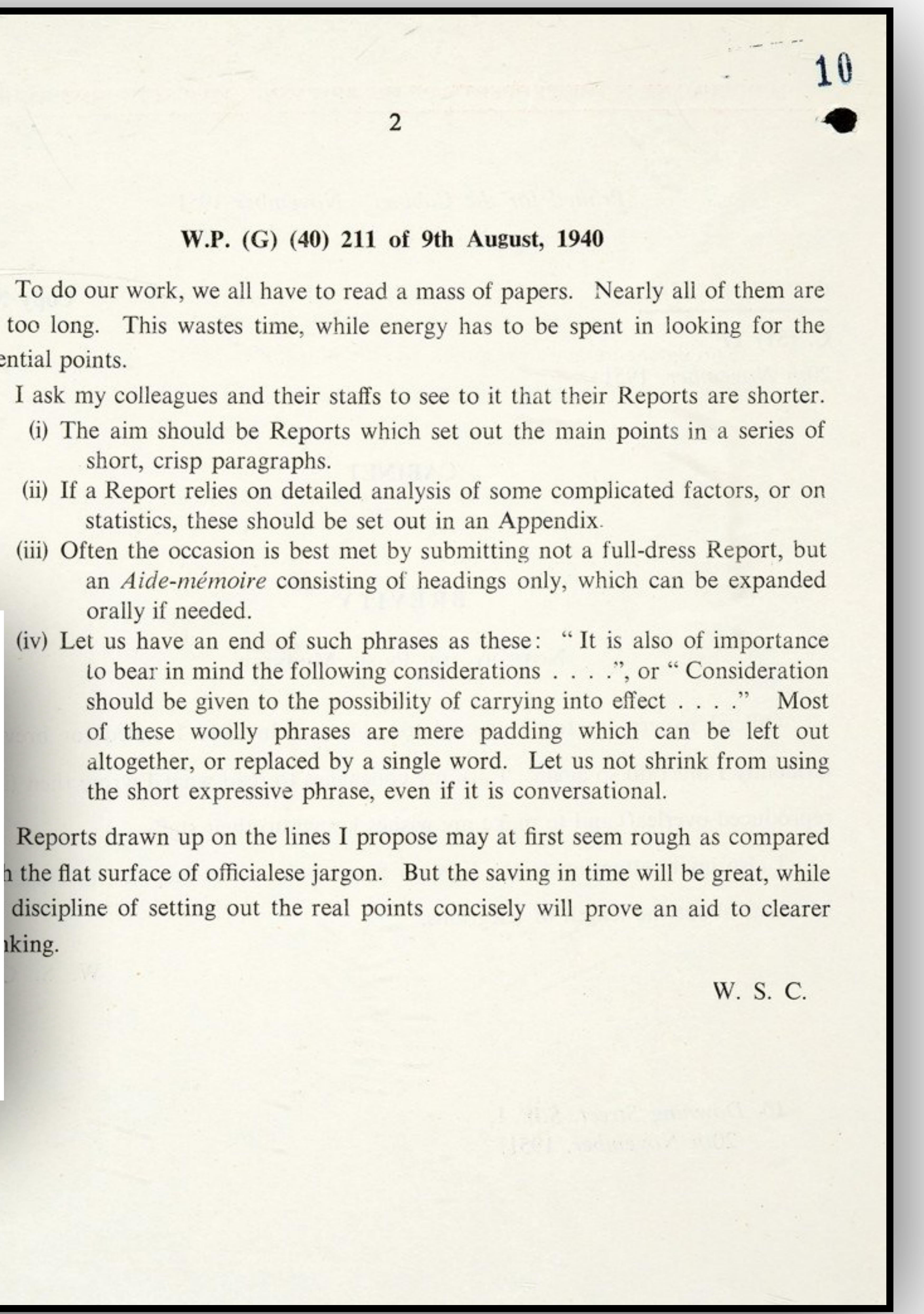


Cabinet Office @cabinetofficeuk · 30 Nov 2016

Winston Churchill was born #onthisday in 1874. Read the writing advice he sent to his officials when he was Prime Minister 📝 #CO100

UK Civil Service

63 1.8K 1.9K



10

2

W.P. (G) (40) 211 of 9th August, 1940

To do our work, we all have to read a mass of papers. Nearly all of them are far too long. This wastes time, while energy has to be spent in looking for the essential points.

I ask my colleagues and their staffs to see to it that their Reports are shorter.

(i) The aim should be Reports which set out the main points in a series of short, crisp paragraphs.

(ii) If a Report relies on detailed analysis of some complicated factors, or on statistics, these should be set out in an Appendix.

(iii) Often the occasion is best met by submitting not a full-dress Report, but an *Aide-mémoire* consisting of headings only, which can be expanded orally if needed.

(iv) Let us have an end of such phrases as these: "It is also of importance to bear in mind the following considerations . . . .", or "Consideration should be given to the possibility of carrying into effect . . . ." Most of these woolly phrases are mere padding which can be left out altogether, or replaced by a single word. Let us not shrink from using the short expressive phrase, even if it is conversational.

Reports drawn up on the lines I propose may at first seem rough as compared h the flat surface of officialese jargon. But the saving in time will be great, while discipline of setting out the real points concisely will prove an aid to clearer king.

W. S. C.

Source: Tweet via UK Cabinet Office.

A modern formula

"Tell me what you know. Tell me what you don't know. And then...tell me what you think...I will hold you accountable."

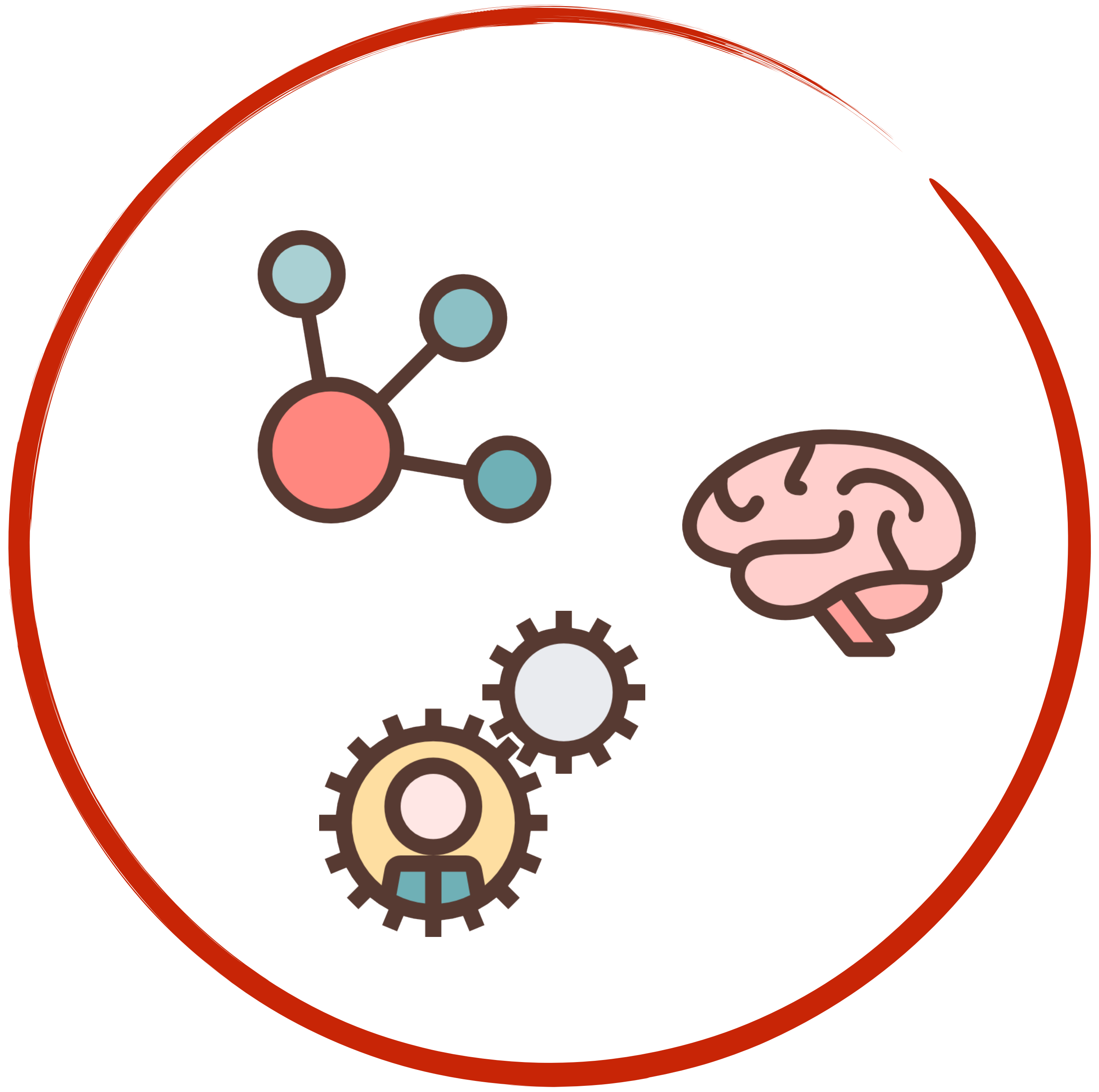
Secretary of State Colin Powell
September 13, 2004, Intelligence Reform Hearing

Source: image from Stephen Voss, TIME magazine.

What you *know*	{ notes, analytic fragments
What you *don't know*	{ information gaps
What you *think*	{ our assessments!

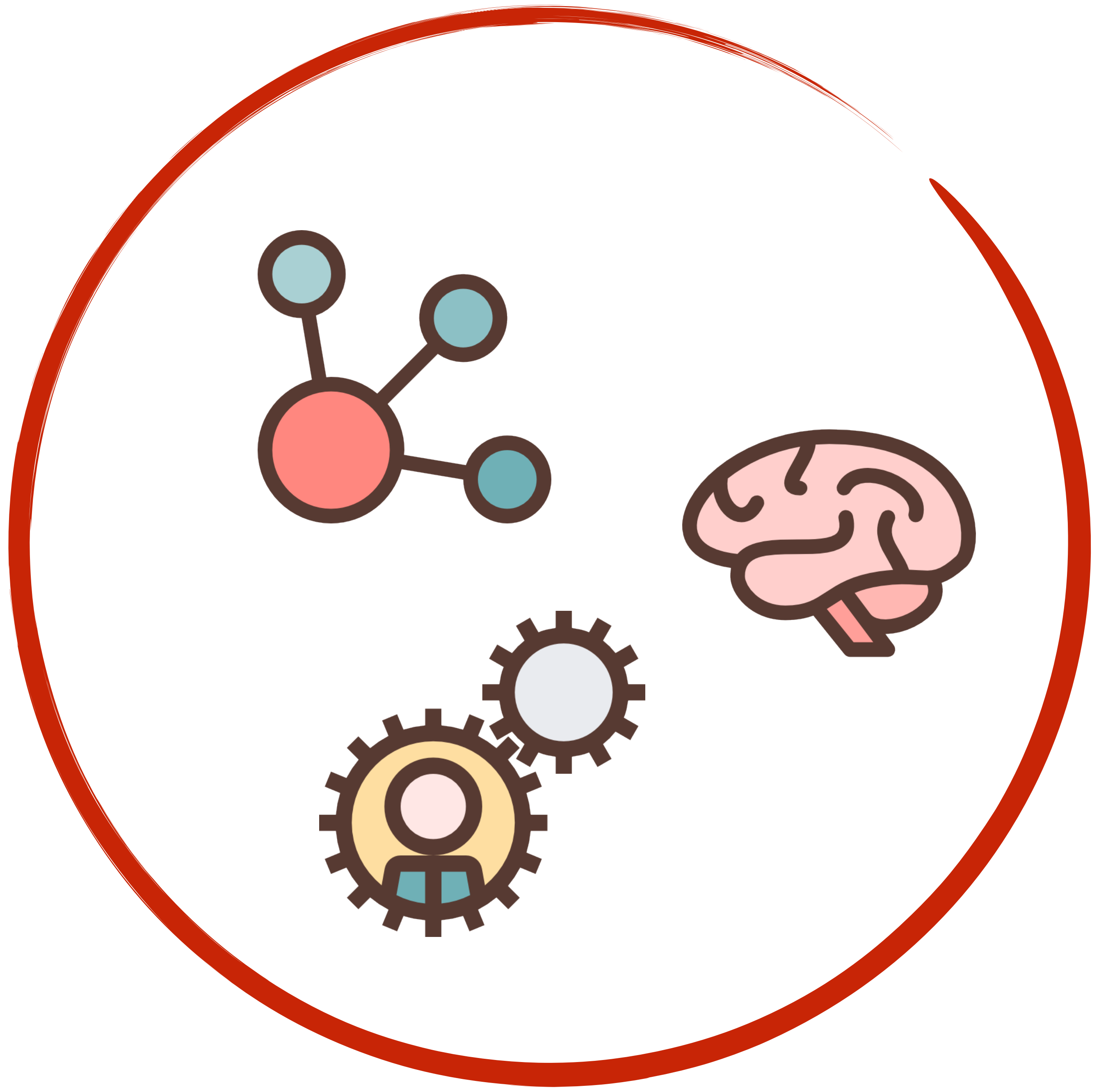
Finished reports...

- memorialize our knowledge of threats
- make knowledge accessible and transparent
- help drive action
- hold analysts accountable
- demonstrate value to the organization



Source: Icons made by Anatoly from www.flaticon.com

Try this tomorrow...



* commit pen to paper
* structure + style + so what
* know + don't know + think
* heed the old school advice!

Source: Icons made by Anatoly from www.flaticon.com

Writing resources…

- Analytic Thinking & Presentation For Intelligence Producers, CIA
- Intelligence Community Directive 203
- The Economist