Applying WWII-Era Analytic Techniques to CTI

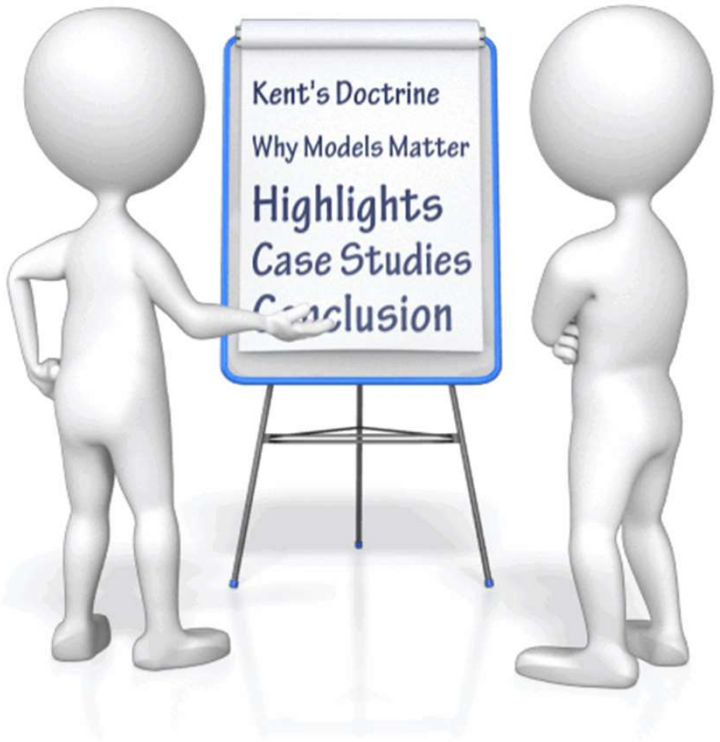
Jake Williams
@MalwareJake

$whoami

- Risk manager, breaker of code, responder of incidents
- IANS Faculty Member
- That guy that did forensics on the Biden laptop…
- Two-time winner of the annual DC3 digital forensics challenge
- Former NSA hacker, Master CNE operator, recipient of the DoD Exception Civilian Service Medal
- Formally endorsed by Russian intelligence
- **Dislikes:** those who call themselves “thought leaders,” “crypto bros,” and anyone who **needlessly adds blockchain** to a software solution

Agenda

- Introduction to Kent's Analytic Doctrine
- Why models matter
- Highlighting "The big four"
- Case studies
- Conclusion



Introduction to Kent's Analytic Doctrine

Just because it's old, doesn't mean it's bad

Kent's Analytic Doctrine

- Kent's analytic doctrine is a model for performing more rigorous and structured analysis
- The doctrine has been taught to formal intelligence analysts by the US (and other countries) for decades
- For some reason, as intelligence moved into the realm of cyber, people seem to have forgotten the lessons learned in traditional intelligence analysis

We do NOT need to reinvent the wheel

- Cyber is new discipline, but it's not so dramatically different from traditional analysis that we need to forget lessons learned

Kent's Nine Steps to Success

1. Focus on Policymaker Concerns
2. Avoidance of a Personal Policy Agenda
3. Intellectual Rigor
4. Conscious Effort to Avoid Analytic Biases
5. Willingness to Consider Other Judgements
6. Systematic Use of Outside Experts
7. Collective Responsibility for Judgement
8. Effective Communication of policy-support Information and Judgements
9. Candid Admission of Mistakes

Why Models Matter

And we're not talking about Vanna White…

Why models matter

People often ask why models matter in the first place

Models provide:

- Repeatability
  - Will the analyst, given identical data, reach the same conclusion again?
- Consistency
  - Will multiple analysts, given the same data, reach identical conclusions?
- Metrics
  - How well does an analysis adhere to the model?
- Rigor/Credibility
  - Is the CTI team just making stuff up?!

CTI has a credibility problem

In speaking with many executives, it is clear that CTI has a credibility problem

There are many reasons for this (far more than we have time to discuss), but models help alleviate that perception

Adopting and adhering to models will help remove some of the credibility problem as models help with consistency and the perception of intellectual rigor

The Doctrine

Nine steps to supercharge your analysis

#1 - Focus on Policymaker Concerns

At the end of the day, every organization is funded by some decision maker who controls a budget

- If an activity isn't providing value to this decision maker, it is unlikely to continue to be funded

Fixing it

- Ask policymakers what's important to them
- Ask for feedback on your reporting
  - How can I make this product more valuable to you
- Understand and respond to drivers at the business unit level

#2 - Avoidance of a Personal Policy Agenda

Leave your agenda out of reporting

- At best it's seen as unprofessional, at worst manipulative

It can be really hard to avoid some personal agenda when writing about topics that personally hit close to home

- I have a hard time writing about Russia…

Fixing it

- Even if it isn't a "personal" agenda, avoid discussing anything that doesn't contribute to the report
- Ask an unbiased reader to assess whether you've included any agenda points in your reporting

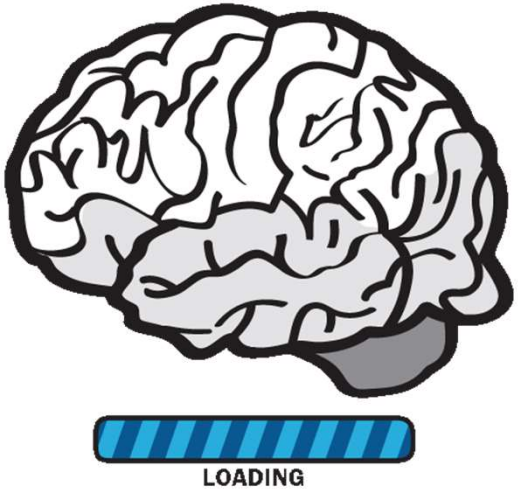
#3 - Intellectual Rigor

CTI reports always rely on analysts to fill in missing information

- Unfortunately, this creates a huge consistency gap in CTI analysis

CTI analysts at many orgs are accused of “making stuff up”

- Whether to their faces or behind their backs



Fixing it

- Use models and structure analytic techniques
- Communicate the use of the models you’re using
- Give credit to others whose work you are building on

#4 - Conscious Effort to Avoid Analytic Biases

Most CTI reports are chock full of analytic biases

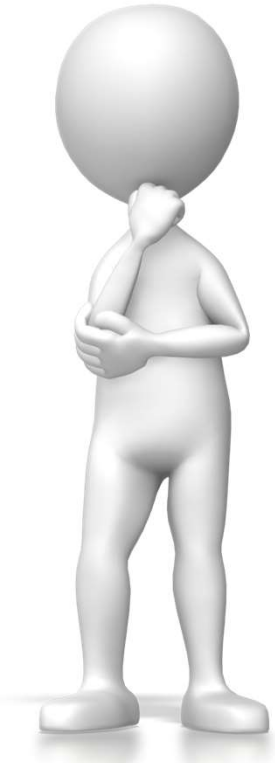
While many “CTI analysts” today are not trained in analytic biases, most executives are

- The GMAT even has a section on analysis and argumentation

Fixing it

- Train your team on analytic biases and logical fallacies so they can call you out when you use them
- Review published reports (including your own) to identify patterns where analytic biases have been used

#5 - Willingness to Consider Other Judgements



Repeat after me: I am **not** always right

There are others on your team with experience that may lead them to a different (and even better) conclusion

Fixing it

- Don't pay lip service to the word "consider"
- This is particularly problematic with managers, where they feel adopting the judgments of subordinates erodes their authority
- ACH can help objectively compare different judgments

#6 - Systematic Use of Outside Experts

Repeat after me: I am **not** an expert in everything

If you're awesome at CTI, someone else in your org is probably better than you at many technical topics – **use them!**

Fixing it

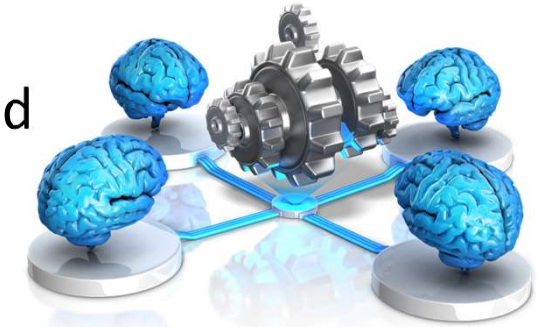
- When organizations focus on team wins rather than individual wins, this tends to be less of an issue
- Facilitate easy access to outside experts – this is incompatible with a six month procurement process to talk to a consultant for an hour
- Network and build your rolodex of experts you can call

#7 - Collective Responsibility for Judgement

A CTI team may disagree behind closed doors, but when a report is issued, the whole team should stand behind it

- When consensus can't be reached, have dissenting parties document their alternate opinion in writing

Don't participate in sharpshooting the report once released

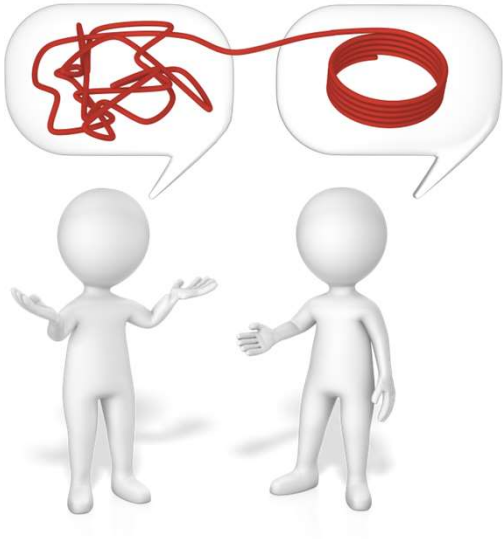


Fixing it

- Yet again, this tends to be less of a problem in orgs where team wins are valued over individual wins
- Instill in all team members that sharpshooting reports outside the team will not be tolerated and will be met with disciplinary action

#8 - Effective Communication of Judgements

Your analysis is worthless if the audience can't understand what you're saying and how you reached your conclusions



Fixing it

- Put time into your executive summary and one-slider presentations for the board – illustrations help **A LOT**
- Get rid of techno-jargon in your communication
- Get a reviewer with similar experience to your audience
- When possible, distill analysis to a few key points for decision makers

#9 - Candid Admission of Mistakes

We all make mistakes – CTI analysts make more of them

In most cases, significant information is missing – we must make judgments about missing information

- Many of those judgments will be wrong…

Fixing it

- Suck it up, nobody likes to be wrong, but we owe it to stakeholders to correct past mistakes (even if they are only based on missing info)
- Foster a culture where issuing a corrected report isn't a big deal - it's far better to get the updated info

The Big Four

Because sometimes you only have one hand to count on…

Kent's Nine Steps to Success

1. Focus on Policymaker Concerns
2. Avoidance of a Personal Policy Agenda
3. Intellectual Rigor
4. Conscious Effort to Avoid Analytic Biases
5. Willingness to Consider Other Judgements
6. Systematic Use of Outside Experts
7. Collective Responsibility for Judgement
8. Effective Communication of policy-support Information and Judgements
9. Candid Admission of Mistakes

Case Studies

Learning from the past to think about the future

Case Study #1 – Use of outside experts

Bletchley Park mistakenly recruited Geoffrey Tandy, thinking he was a cryptogrammist (a code breaker) when in fact he was a cryptogamist (a botanist who studies plants without seeds)

When Bletchley recovered a water logged codebook, the code breakers believed it to be a total loss

- Tandy knew better since “drying out organic material” is core cryptogamist…

This success starts with a mistake, but without Tandy being in the right place already, this would have been a missed opportunity

Case Study #1 – Use of outside experts

Too often in CTI we are faced with unfamiliar technology and cultures that are foreign to us

Part of this problem can be solved by building in diversity on your teams

- Diversity in backgrounds and experience are most important here

Empower CTI teams to readily connect with experts outside the organization by building relationships before critical events

Case Study #2 – Admission of mistakes

When the US entered the war in 1942, the British Navy already understood the importance of using convoys to protect ships

They even had good data on how convoys protected shipping assets

Fleet Admiral Ernest King believed the British Navy was “obsolete and incompetent” and decided not to follow their advice on the use of convoys

- Some also attribute this to a lack of escort ships in the Atlantic Fleet

King eventually reversed course, admitted the shortcoming, and used escort ships to protect the convoys

Case Study #2 – Admission of mistakes

A lack of available escort ships (a resourcing issue) and lack of confidence in the Royal Navy (a reputation issue), influenced King's decision to ignore the advice of his peers

All too often, CTI suffers from similar issues:

- Ignoring or diminishing valuable reporting because of a personal bias against the source
- Knowing the "correct" course of action, but being limited in response options because of inadequate resourcing

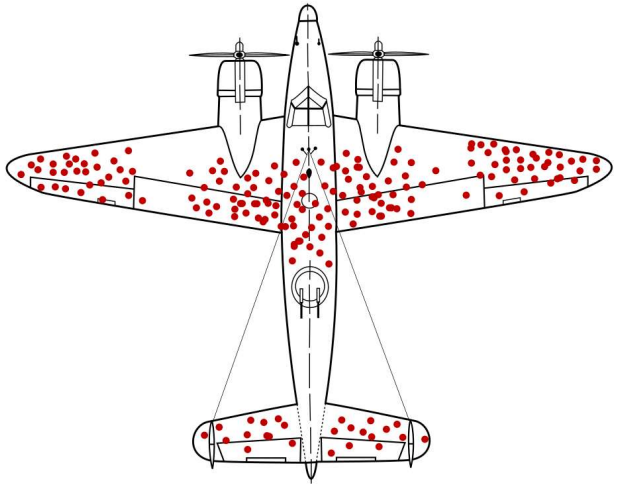
Case Study #3 – Analytic Biases

WWII engineers studied the aircraft returning from battle to see where they were being hit and adjusted to add armor to those locations

The thought process was that the locations where the planes were observed being hit were the most likely to be struck by anti-aircraft fire

The statistician Abraham Wald recognized an important survivorship bias that was present in the data, noting that planes which suffered fatal hits never returned and as such were not part of the analysis

- **Conclusion:** The wrong parts of the aircraft were receiving extra armor



Case Study #3 – Analytic Biases

In CTI, analytic biases prevent us from making rational judgments about the data that is actually available

- Sampling bias often contributes to inaccurate pictures of data
- Anchoring bias leads teams to focus on the data acquired early in the investigation, forgoing better leads that are discovered later
- Illusory correlations are performed because two unlikely events happening nearby “can’t be a coincidence”
- Hindsight bias hampers our ability to predict the most likely attacks

Case Study #4 – Avoidance of a Personal Policy Agenda

German Generals believed* the Russians:

- Would only commit their Western forces to defense
- Their tanks were superior to anything the Russians could produce

Hitler is widely thought to have believed these and he removed Generals who didn't agree with his narratives

Telling leaders what they want to hear so you can be favored is clearly advancing their personal policy agenda

- And your personal policy agenda too…

Case Study #4 – Avoidance of a Personal Policy Agenda

CTI reports, and to a larger extent incident response reports, are often written to justify the adoption of some initiative

- "If we'd had X (that I conveniently advocated for), then the incident wouldn't have happened"

It can sometimes be difficult to distinguish between legitimately good reporting and a personal agenda

- When in doubt, get an unbiased party to review the report, with a specific eye for a personal agenda

Case Study #5 – Effective Communication

When Germany invaded France in 1940, the German tank commanders considered their radio communications one of their most important assets

- Some German commanders are reported to have considered radio drills at least as important (if not more so) than gunnery drills

Most French tanks lacked radios

- Most of the French infantry units didn't have radios either – they were primarily passing intelligence and orders via courier (and telephone in some cases), inhibiting their ability to quickly adapt

Case Study #5 – Effective Communication

Just as ineffective communication hampered the French, in CTI it hurts our response efforts

Generally ineffective CTI communication takes three forms:

- Communication comes too late
- Not enough context to action the information
- The information is targeted at the wrong audience

Process adjustments can fix the first two, the last requires a feedback process for intelligence reporting

Conclusion

Let’s wrap this up...

Conclusion

Don’t reinvent the wheel with CTI analysis

CTI analysts can make the same use of Kent’s analytic doctrine that traditional intelligence analysts have for decades

Adopting the nine (or even just four) steps in the doctrine will help CTI teams perform more consistent analysis

@MalwareJake