Levels of Threat Intelligence

SANS CTI Summit 2016

2016-02-03

Michael Cloppert
LM-CIRT

The Struggle is Real

My challenge:

Convey academic concepts to detail-oriented, technically proficient practitioners who might be skeptical that simple concepts can subconsciously and profoundly influence cognition.

Bias is a natural heuristic – a short-cut, or simplification, our brains use to interpret our environment.

These ideas are basic; their imprecision is deliberate. They are controlled biases, where the degree to which they improve our understanding of adversaries is the primary measure of success.

Levels of Threat Intelligence - Overview

- **Concept:** Degrees of abstraction, like those in established intelligence disciplines, clarify how we think about our own.

- **Background / motivation**
  - A FOR578 student asked about the JP 2-0
  - I felt stupid and read it
  - I thought “meh”
  - I read it again
  - My brain did a thing and felt funny
  - I did some research
  - My thinking about CTI became much more clear

The military did something smart

Who Dis Iz?

Hints:

- **Was a BAMF**
- **Was Prussian**
  - **(that means German, -ish)**
- **Wrote a book on war**
  - **Not Sun Tzu, though I see the resemblance**
  - **Literally, titled *On War***
- **Military theoretician, ideas survived emergence of:**
  - **Mechanized warfare**
  - **Air combat**
  - **Chemical, biological, nuclear weapons**

Carl von Clausewitz

So what?

Dude's been around awhile…
his theories are quite old!

Growing Pains in CTI

The primary purpose of any theory is to clarify concepts and ideas that have become entangled.
- Carl von Clausewitz

- Intel-driven CND has grown tremendously
  - Our intelligence corpus
  - Our models and their dependencies, relationships
  - Our capabilities
  - Our workflows
- We now have a spectrum of all of these
- The spectrum has caused mis-communications, confusion, conflict
- Our domain is so complex, we have experienced entanglement
- We need a simpler way to think about this complexity

von Clausewitz: Relevant Theory

- Introduced concepts of **tactical** and **strategic** levels of war
- Alluded to application of strategy as "**operations**"
- Provided basis for levels of war used through today:
  - Tactical
  - Operational
  - Strategic
- Established intelligence studies borrow from / mimic this
- Intelligence, defined…
  - "every sort of information about the enemy and his country – the basis, in short, of our own plans and operations" – von Clausewitz, *On War*

http://www.clausewitz.com/readings/Echevarria/APSTRAT1.htm

And?

Despite being over 200 years old, theories have withstood major changes in capabilities and remain relevant…

if these theories are applicable to us, they will stay applicable to us!

JP 2-0: Joint Intelligence

- 2013 publication written under orders from CJCS Dempsey
- “Guidance for conducting … intelligence activities across the range of military operations”
- Defines Tactical, Operational, Strategic intelligence levels
- Is collective paradigm for intelligence within U.S. military

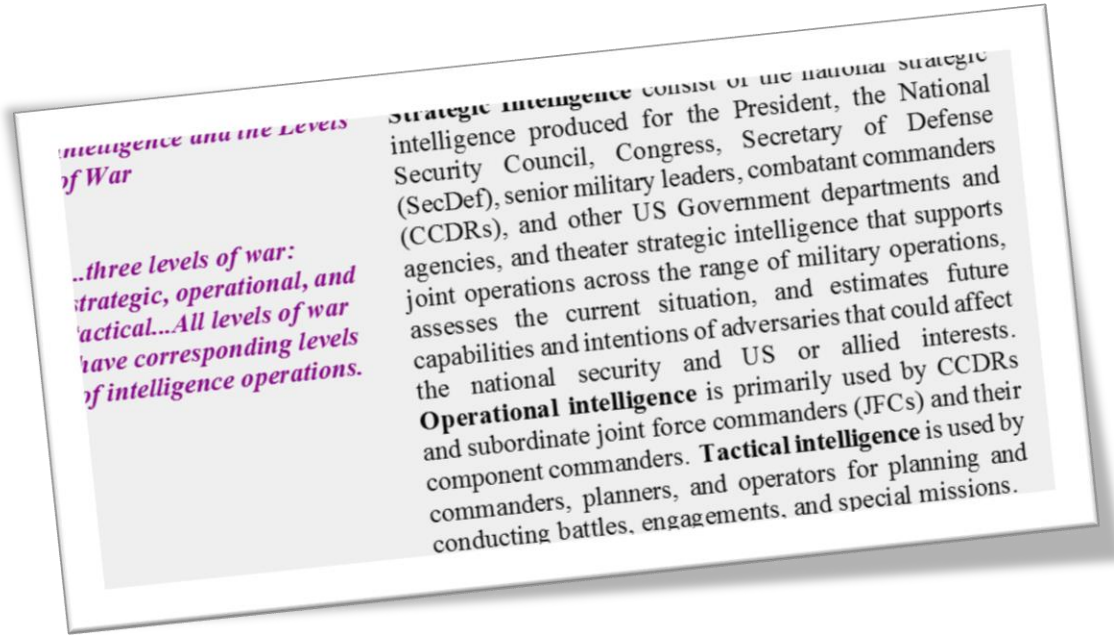
- **LET’S ~~STEAL~~ i mean BORROW IT!**

JP 2-0: Caveats, Considerations

- Document is much more than this presentation
- Provides other applicable concepts
  - Will you be attending vol. 4? ;-)
  - Other stuff, maybe?
- Provides insight into how your country's military operates at high level
- Our focus is one concept at a time

JP 2-0: Intelligence and the Levels of War

- **Strategic**
  - **Consumers**
    - **POTUS**
    - **NSC**
    - **Congress**
    - **SECDEF**
    - **CCDRs**
  - **Assessments**
    - **Effects on national security of US, allies**
- **Operational**
- **Tactical**

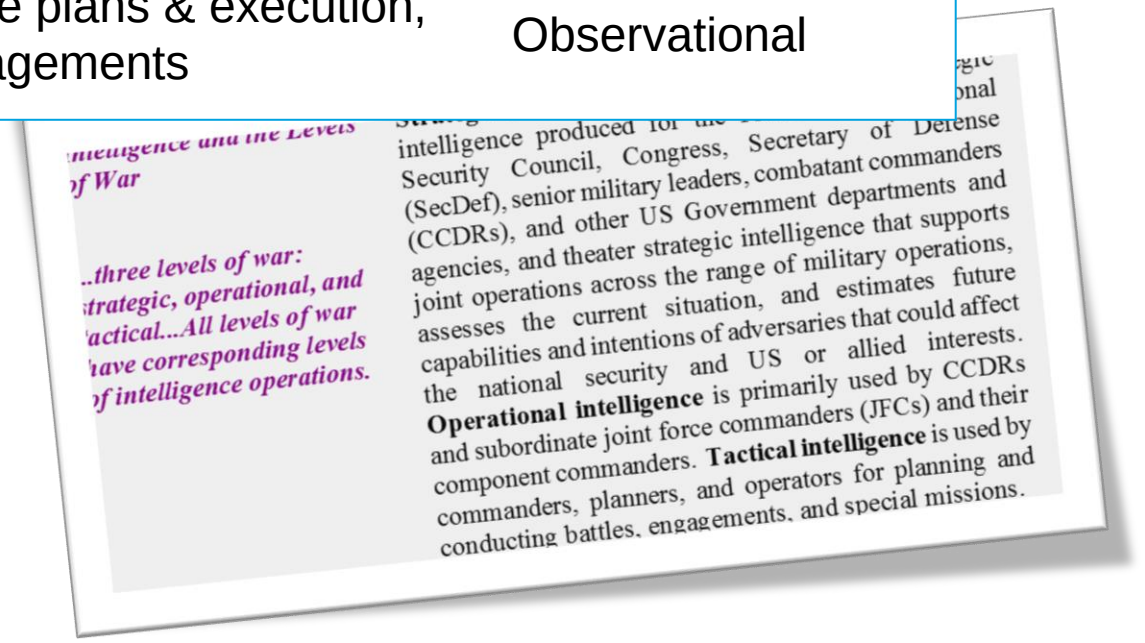


...three levels of war: strategic, operational, and tactical...All levels of war have corresponding levels of intelligence operations.

intelligence produced for the President, the National Security Council, Congress, Secretary of Defense (SecDef), senior military leaders, combatant commanders (CCDRs), and other US Government departments and agencies, and theater strategic intelligence that supports joint operations across the range of military operations, assesses the current situation, and estimates future capabilities and intentions of adversaries that could affect the national security and US or allied interests. **Operational intelligence** is primarily used by CCDRs and subordinate joint force commanders (JFCs) and their component commanders. **Tactical intelligence** is used by commanders, planners, and operators for planning and conducting battles, engagements, and special missions.

JP 2-0: Intelligence and the Levels of War

	Consumers	Effects	Product Type
Strategic	POTUS, NSC, Congress, etc	US, allied nat'l security	Anticipatory
Operational	CCDRs, JFCs	Capability selection, collection prioritization	Interpretive
Tactical	Commanders, planners, operators	Battle plans & execution, engagements	Observational



JP 2-0: Every level matters!

Principles of Joint Intelligence

(OE: Operational Environment)

Perspective

Intelligence analysts should strive to understand all relevant aspects of the OE. This understanding should include not only the adversary's disposition, but also the sociocultural nuances of individuals and groups in the OE.

Intel-driven CND / “Cyber Threat” Intelligence Levels

	Consumers	Effects	Product
Strategic	Executives, BAISOs	Business strategy risk calculus	Nation-state **Threat Assessments**
Operational	CIS, CIRT, customers, some peers	Investment priorities, capabilities, comprehensive intel, data access	**Campaign analysis**
Tactical	CIRT, partners	Mitigations, detections, “IR”	**KC completion**

In our domain, we can generally think of the levels thusly:

- **Strategic** **Nation-state**
- **Operational** **Campaign**
- **Tactical** **Intrusion**

Intelligence and Command

Intelligence flows up

1. Intrusion
2. Campaign
3. Nation-state

Command flows down

1. Business decisions, needs
2. Collection, processing, assessment capabilities
3. Alerts, workflows

Implications to IR Teams

- **Org responsibilities, products**
  - **Part of team mission statements**
- **Illustrates value of analysis at every level**
  - **Answers some questions about relevance**
- **Work may be prioritized independently per level**
  - **Avoids some aforementioned conflicts**
- **Analyst perspectives better understood**
- **Provides another facet of staffing levels**
  - **Many of us are tactical**
  - **Some are operational**
  - **Few are strategic**