



# Data to Decision Making: All Source Intelligence and Network Data

Leo Gentile  
JFHQ DODIN J2, Technical Director  
15 May 2019



# All Source Intelligence Analysis for Cyber





# Current Situation

- Disparate Data: Lack of access to all data sources
- Numerous Independent Data Sources:
  - Intelligence Community
  - 43 x DOD organizations (network data)
  - 5 x JFHQ-C & CNMF gathered data (C-ISR/C-S&R)
  - Commercial data
- Approx. data amounts- Data analytics unachievable without machine help
- Patchwork policies concerning security, transportation, storage, and usage of data
- Customers & their production requirements not clearly defined



# The Intelligence Issue: The Analyst's Paradigm

- Focus on consolidated serialized reports/output
- Minimal/low understanding of computer network data
- Familiar with intelligence message traffic/databases
- No holistic thread connecting data sources/perspectives, produces uncoordinated & incomplete analytics
- Self programmed boundaries restrict capability and technology development



# Data

- Addressing data governance issues
  - Intelligence community, policy, operations, and development
  - Data Access, Tagging, Formatting, Source connectivity
- Gaining understanding and access to Data at all levels and classifications
  - Tier 1 – Internet Access Point
  - Tier 2 – JRSS Stacks
  - Tier 3 and below – End Point Data
- Data specific staff education
  - Defensive network appliances production and conditioning





# Storage

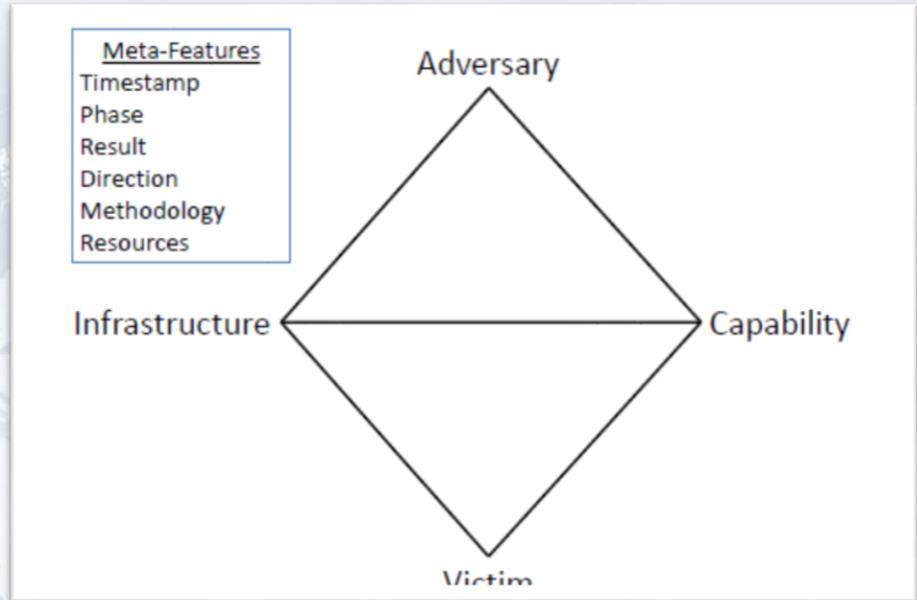
- Still in discovery mode
  - New locations of data everywhere; but data is being stored
- Working with USCYBERCOM to interconnect data source
  - DODIN data structure still in development
- Still trying to gain grasp on storage requirements for “intelligence”
  - Limited guidance on storage of data related to Insider Threat Activity
  - All-Source analysis of enemy activity on blue force network
  - Concern regard the mix of PII with network data and intelligence





# Analytics

- Analytics needed to enable machine learning and artificial intelligence
  - “Fusion” is a good start
  - Basic analysis to identify indicators of compromise (IOC)
  - Identifying patterns of activity
  - New IOCs and Predictive Analysis
- Move past intrusion set and into individual actor pattern of activity



Data

Storage

Analytics

Display

Decision



# Display

## Current

- The Traditional Intelligence “Book Report” style format
- Defensive cyber community recognize as too slow
  - Appropriate for holistic response to acquisition community

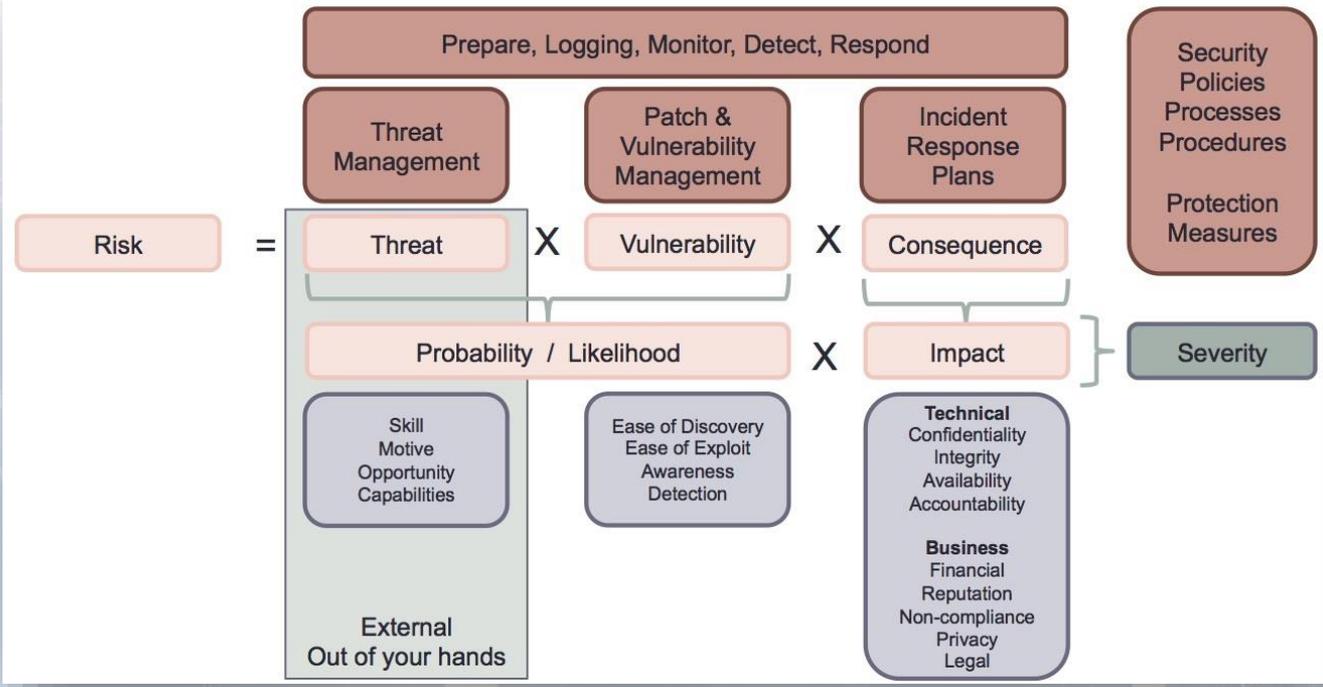
## Future

- Dynamic Display
- Cyber situational awareness: geographic and logical format
  - Integration of cyber into the other domains of warfare





# Decision





# Conclusion

- Cyber All Source Intelligence Analysis is still developmental-
  - Must include more technical details to understand specific targets, techniques, procedures, and trending
- Work cannot be conducted in a void, intelligence must play with others
- Data fusion must be fully integrated into “All Source Analysis” standard
- Intelligence is key in defensive cyber decision making;
  - Vision must expand; cannot work solely within traditional “intelligence” lanes



Questions?

**Leo Gentile**  
**JFHQ DODIN J2, Technical Director**  
**15 May 2019**

visit us

DISA  
Booth **1929**

follow us



Facebook/USDISA



Twitter/USDISA

meet with us

Industry partners can request a meeting with DISA by completing a form at [www.disa.mil/about/industry-partners](http://www.disa.mil/about/industry-partners).