Forensics, Fighter Pilots and the OODA Loop: The Role of Digital Forensics in Cyber Command and Control

By

Heather Dussault, Chet Maciag

Presented At

The Digital Forensic Research Conference

DFRWS 2004 USA Baltimore, MD (Aug 11th - 13th)

DFRWS is dedicated to the sharing of knowledge and ideas about digital forensics research. Ever since it organized the first open workshop devoted to digital forensics in 2001, DFRWS continues to bring academics and practitioners together in an informal environment. As a non-profit, volunteer organization, DFRWS sponsors technical working groups, annual conferences and challenges to help drive the direction of research and development.

http:/dfrws.org

Forensics, Fighter Pilots and the OODA Loop

The Role of Digital Forensics in Cyber Command & Control

Heather M.B. Dussault, Ph.D.
Assistant Professor, Electrical Engineering
SUNY Institute of Technology
and member of the Griffiss Institute

The Role of Digital Forensics in Cyber C2

- An Introduction to the OODA Loop and Command and Control
- Comparison of Forensic and C2 Processes
- Implementing Digital Forensic Processes in Cyber Command and Control Processes

Acknowledgements

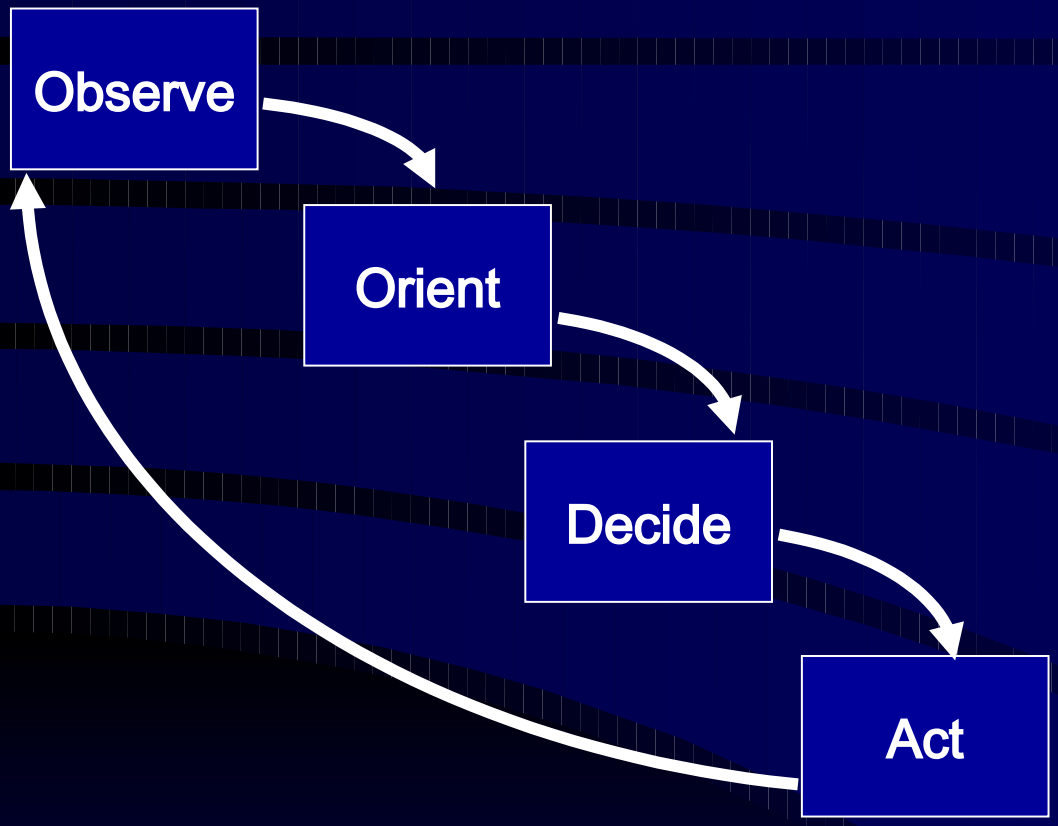
- Chet Maciag, Cyber Operations Branch, Air Force Research Laboratory

- Mike Medley, Dept. of Electrical Engineering, SUNYIT, Principal Investigator, Spread Spectrum Analysis for Next Generation Intrusion Detection, sponsored by the Air Force Research Laboratory and Air Force Office of Scientific Research

Dogfights and Fighter Pilots
- An Analysis by Col. John Boyd circa 1987-

- What made the difference between winning and losing?

Boyd's OODA Loop

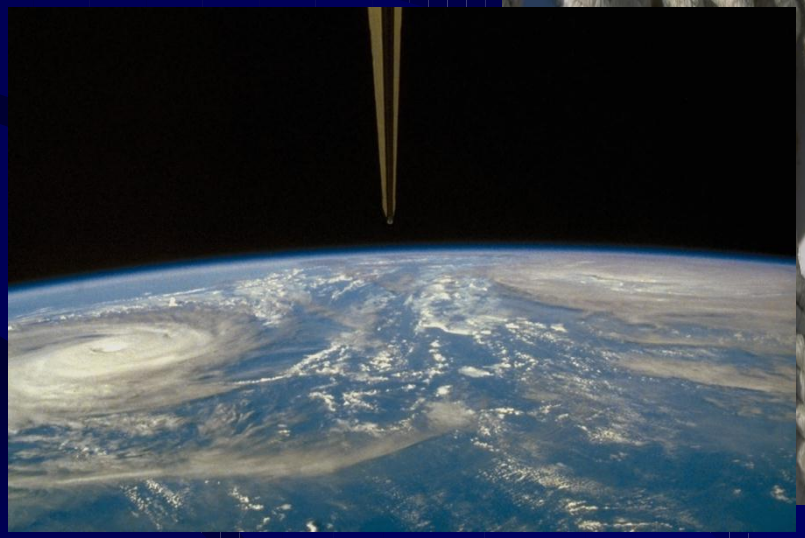


- Iterative process
- People, not machines, are the initiators and participants
- Informed decisions are coupled to actions
  - Proactive
  - Timeliness of response and loop processing are critical

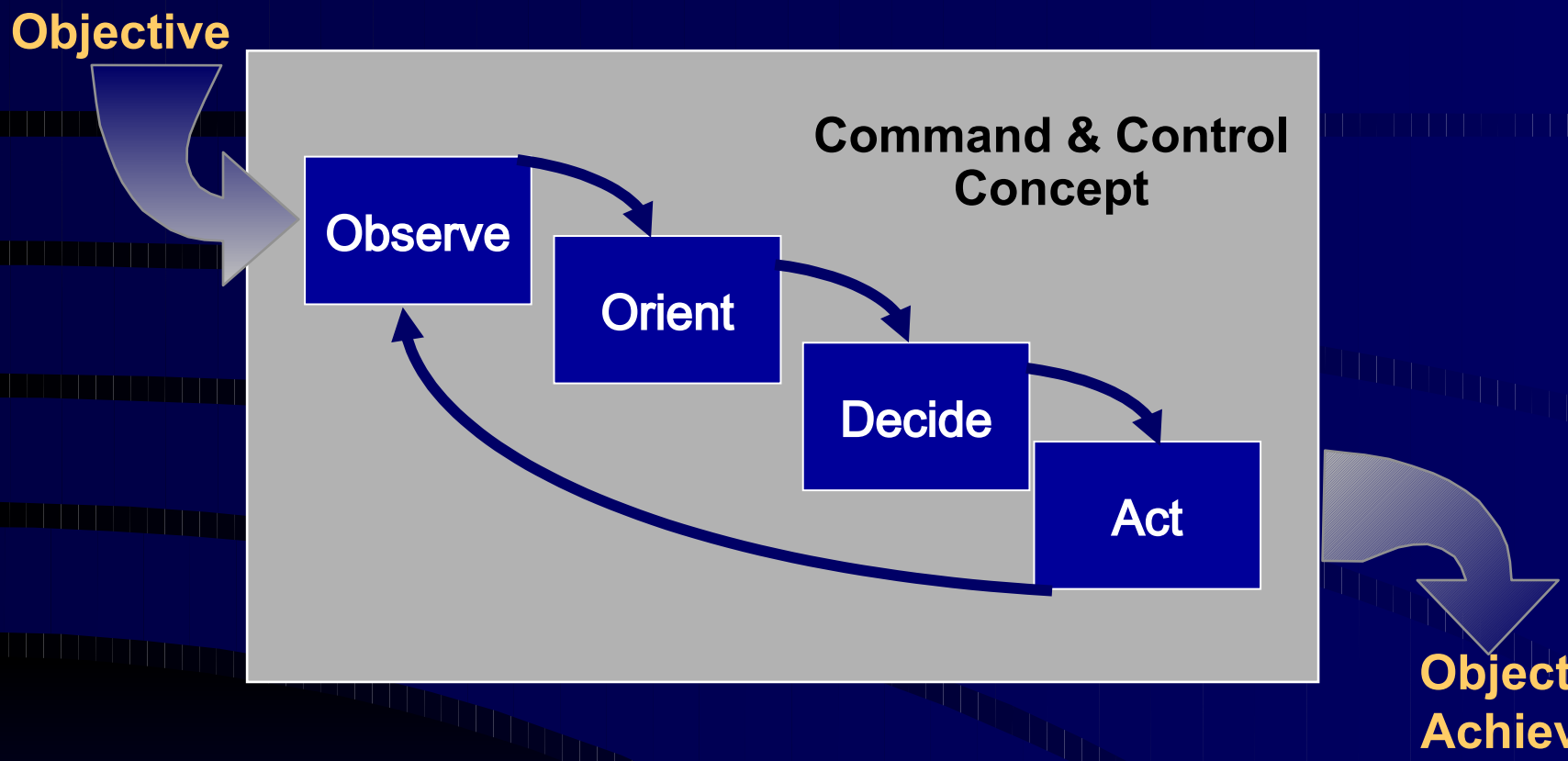
Keys to success: Disrupting your opponent's OODA loop or completing your OODA loop faster than your opponent

Command and Control

- Two general phases:
  - Planning: deliberate and crisis-action
  - Execution
- Command and control process attributes
  - Iterative
  - Multi-threaded
  - Dynamic and flexible
- Assets / Resources
  - Personnel
  - Equipment
  - Communication
  - Facilities
  - Procedures



OODA'ing is a Fundamental Command & Control (C2) Process



1. Collect information to determine if objective is achieved →
2. Build the operational picture (create situational awareness) →
3. Develop/reassess courses of action and priorities →
4. Execute the selected course of action → (go back to step 1)

Cyber Command & Control (C2)

- Computer and information systems are widely used in C2
  - Part of the C2 weapons system
  - Highly capable with many applications
  - Global enterprise
  - Complex connectivity
  - Difficult to monitor
  - "Target rich" environment

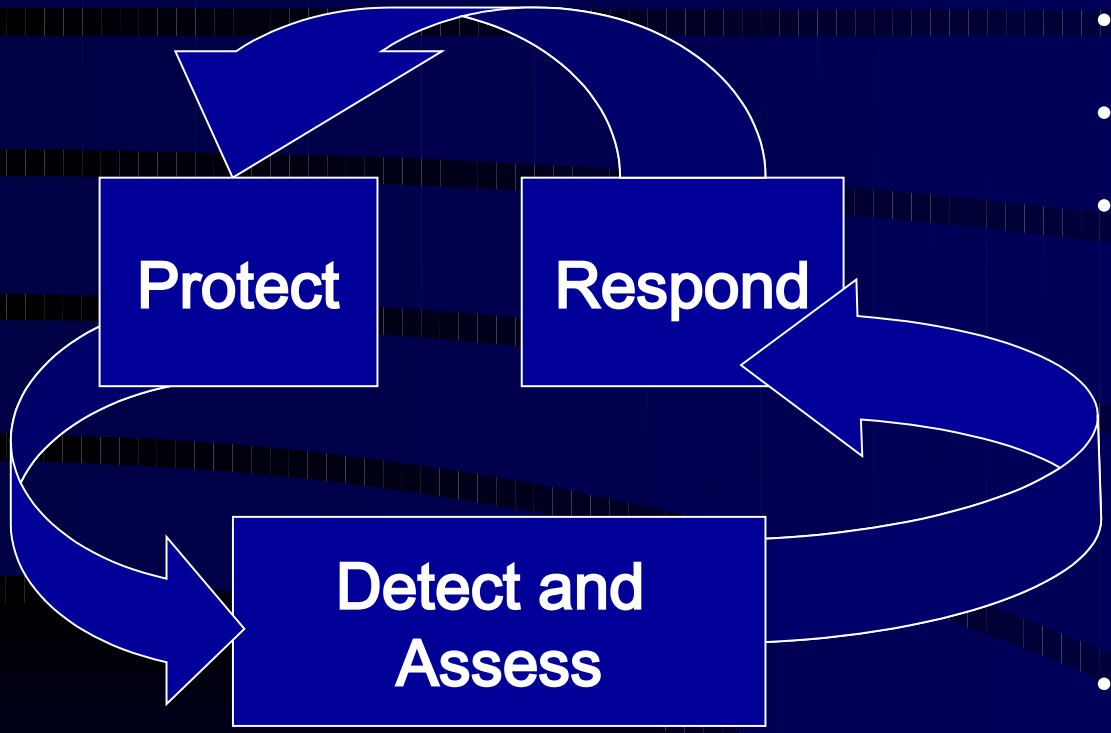
- Need to effectively plan and execute computer and information system operations and defenses (otherwise, cyber C2 may have a lengthy OODA cycle)

- Cyber situational awareness is a critical component in cyber C2

Cyber Situational Awareness
- A First Step -

Federal Information Security Act "Report Card"	Potential Cyber C2 Responsibilities
Full inventory of critical assets	Organize, train and equip functions and combatant commander planning
Identify critical infrastructure and mission critical systems	Combatant commander must identify and marshal of assets for a mission
Strong procedures for incident identification and reporting	**Forensic capabilities in cyber C2 planning and execution**

Cyber Situational Awareness - PDAR Loop-



- Defined in AFDD2-5
- Iterative
- Focus on up-front protection of resources
  - Policies
  - Procedures
  - Mechanisms
- Reactionary → Respond to detected actions /events

Comparing Processes

Digital Forensic Science Process	OODA Loop	PDAR Cycle
		Protect
		Detect
Identification	Observe	Detect/Assess
Preservation	Observe	Assess
Collection	Observe	Assess
Examination	Observe/Orient	Assess
Analysis	Orient	Assess
Presentation	Orient	Assess
Decision	Decide	Respond
	Act	Respond

A Missing Link in Forensic Process for Cyber C2: Act

- Defined digital forensic science process maps well into conventional C2 observe, orient and decision processes
- Forensics isn't currently thought of as a "dogfight" → link to rapid action and reiteration isn't there
- The OODA loop stresses:
  - Time is a critical element in determining outcomes
  - Informed decisions are coupled to rapid actions
  - People are initiators
- Cyber threats require rapid reaction times (Howes, et al , 2004 and Laurie, 2004)

Digital Forensics and Dogfights

- When faced with a cyber threat or blended threat, commanders and command staffs need to know
  - What could happen (observe)
  - What are the hallmark signatures of an event (orient)
  - What is the source and extent of an event (orient)
  - What may happen next (orient)
- Cyber C2 couples informed decisions with actions
  - Proceed with the best available course of action (decide)
  - Act quickly and know/ look for indicators of success (act)

Key to success: Digital forensic mechanisms, processes and operations must be an integral and continuous part of cyber C2

Implementing Digital Forensic Processes in Cyber C2

- Capture minimal essential elements of forensic information for the C2 system
  - What are the "black box" essential elements? (Heath & Woodcock, 2000)
  - Collection rates & periodicity
  - Allowed levels of abstraction or compression
  - Means of authentication and assuring integrity
- Maintain and present cyber situational awareness for a dynamic, global enterprise
- Provide trusted storage of forensic information
- Support remote forensic monitoring, reporting and analysis without providing another means for attacking the system (Laurie, 2004)
- Provide rapid analyses

Planning Considerations for Digital Forensics in Cyber C2

- People must be selected, trained and available to support digital forensics
- Role of humans in the OODA loop for cyber C2 needs to be critically examined
  - Human-machine interactions
  - Cognitive models
  - Behavioral profiles
- Solutions must be scalable
- Cyber situational awareness should not be separated from "kinetic" situational awareness or abstracted to meaningless content
- Reliable, remote, distributed network monitoring required
- Adopt standard, accepted practices and procedures
- Procedures must be in place prior to their need and continuously and correctly used

Opportunities for Implementing Digital Forensics in Cyber C2 Systems

- Forensics for planning
  - Course of action development for deliberate and crisis action planning based upon law enforcement scenarios and lessons learned
  - Course of action analysis:- has the plan "made its case"

- Forensic support for rapid decision making
  - Establish criteria for decision-quality information based upon forensic practices and standards
  - Cyber attack indications and warning capabilities would be a natural outgrowth of continuous, integrated forensic analysis as part of cyber C2

More Opportunities for Implementing Digital Forensics in Cyber C2 Systems

- Forensics processes in predictive battle management
  - Forensically identify expected behaviors and observable responses and messages for a given C2 system
  - Support battle damage assessment
  - Support effects based operations
  - "Get inside" the adversary's OODA loop
- Forensics in wargaming, critical experiments and military exercises

In Summary

- Digital forensic science process maps well onto observe, orient, and decision processes of C2
- Is digital forensic science equipped and ready to enter the dogfight for cyber C2?
- Opportunities exist for inserting digital forensics in C2 processes
- Technical issues will need to be addressed
  - Identify minimal essential elements of forensic information for Cyber C2
  - Provide scalable solutions
  - Adapt and develop trusted methods for continuous forensic analysis in time-sensitive environments