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

Heather M.B. Dussault
SUNY Institute of Technology and The Griffiss Institute for Information Assurance

Chet J. Maciag
Defensive Information Warfare Branch
Air Force Research Laboratory, Information Directorate

Abstract

Derived from personal observations of the differences between winning a losing a dogfight, the ability rapidly move through a decision cycle of observing, orienting, deciding and acting (*i.e.,* Boyd's OODA loop) is a central concept in modern military command and control (C2). The OODA loop, the digital forensic science process, and protect-detect-assess-respond processes are briefly described, compared and contrasted. The first three steps of the OODA loop (observe, orient, and decide) map reasonably well onto the digital forensic science process and indicate that many digital forensic tools and techniques may well find use in cyber command and control processes. Attributes of digital forensic processes suitable for implementation in cyber C2 systems are described and implementation issues are discussed. One thing that was missing in the digital forensic science process that was present in the OODA loop is the link from decision to action. In establishing digital forensics capabilities in cyber C2 systems, the potential to establish links between decision-making and actions would naturally exist and allow digital forensics to expand into new capacities and capabilities in such broad areas as planning tools; decision support; wargaming, exercises and experiments; and predictive battle management.

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

Heather M.B. Dussault[1]
SUNY Institute of Technology and The Griffiss Institute for Information Assurance

Chet J. Maciag
Defensive Information Warfare Branch
Air Force Research Laboratory, Information Directorate

Introduction

Col. John R. Boyd wanted to understand how fighter pilots win or lose dogfights. [1] Col. Boyd wanted to know why F-86 fighter pilots often defeated MiG-15 fighter pilots in a dogfight, even though the MiG-15 could was an aerodynamically more maneuverable aircraft than the F-86. One of the major points of Boyd's observation in describing how a fighter pilot operates and wins dogfights his description of the OODA (Observe-Orient-Decide-Act) loop. Boyd observed that what made a significant difference in the outcome of a dogfight was how quickly individual pilots could go through the OODA loop and "move ahead" of their opponents or execute their selected mission plan/strategy [2]. Sometimes the deciding factor is technology; sometimes it's the human-technology interface; and sometimes it's the human thought process. In the case of the F-86 and the MiG-15, Boyd's theory was that the difference in the pilot's OODA loops was that the MiG-15 with its manual flight control took a little more effort and a little more time for the pilot to interact with than did the F-86's hydraulic flight control system [2]. The better human-technology interface of the hydraulic flight control, resulted in an easier workload for the human, faster cycle time through the OODA loop, and more wins in dogfights – where, much like computer network attacks and crimes, a lot of "very bad things" can happen in tenths of seconds.

There are two important features to notice about the OODA loop: 1) the loop is an iterative process; and 2) people, not machines, are the ultimate initiators and participants in any "dogfight." All three elements: technology; human-machine interface; and human performance, can contribute to time required to move through an OODA loop cycle, creating the differences between failure and success. Boyd's OODA loop has been extensively applied to traditional military command and control processes and systems and extended to fields such as business competitions, tactical police work and software development [2]. The notion of being able to operate "inside an opponent's decision cycle", or move through the OODA loop faster than an opponent, is viewed as a critical precept to success in operations, whether it is in a dogfight, other military operations, bringing a product to market, or winning a sporting contest.

Military Command and Control (C2)

When it comes to continuous operations and vigilance required of command and control operations, the roots of the OODA loop in a "dog fight" provide an interesting parallel. Command and control (C2) is defined as: "The exercise of authority and direction by a properly designated commander over assigned forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communication, facilities, and procedures employed by a commander in planning, coordinating, and controlling forces and operations in accomplishment of the mission." [3] Command and control processes are dynamic and flexible and bring a variety of people, tools, and procedures to bear as part of prosecuting a mission. That mission may be as large as a major campaign, a continuing mission of surveillance and monitoring for treaty compliance purposes, a peacekeeping mission, an air-to-air encounter (the "dogfight"), the prosecution of a time-critical target such as a mobile SCUD launcher, a humanitarian relief mission or a wide variety of other major and smaller missions.

Each mission requiring command and control also has two general phases: a planning phase and an execution phase. Planning may be characterized as deliberate (well in advance of execution) or time-sensitive / crisis-action planning. In brief, during planning, the commander takes his or her intent (*i.e.,* what constitutes a successful mission) and identifies the necessary personnel, equipment, communication, facilities and procedures to satisfy the mission objectives and develop and evaluate possible courses of action (COAs). The execution phase begins after a commander disseminates an approved plan and appropriate orders are issued to engage the plan into action. As execution occurs, the commanders assess the effects of the execution on achieving mission objectives and replan or choose alternate courses of action as required. As is often said, the first casualty of any engagement is the plan itself. And that's where the OODA loop plays a pivotal role in command and control – whether it is for the more conventional "kinetic" warfare, asymmetric warfare represented by computer network attacks, or blended threats.
The OODA loop, as shown in Figure 1, illustrates the flexible and dynamic nature of command and control and the need to ***quickly*** respond to changing conditions to be able to successfully meet mission objectives. Network-centric warfare / computer network operations

The computer and information systems used as part of the command and control structure to accomplish a military mission are considered a weapons system. Network and networking capabilities are viewed as so vital to the conduct of military missions that the catch phrase and concept of "network centric warfare" and network centric operations" have become part of the mainstream of military command and control vernacular. Knowing network status (an as yet to be consistently defined qualitative or quantitative metric) is vital to operations and the ability for a commander to achieve mission objectives.

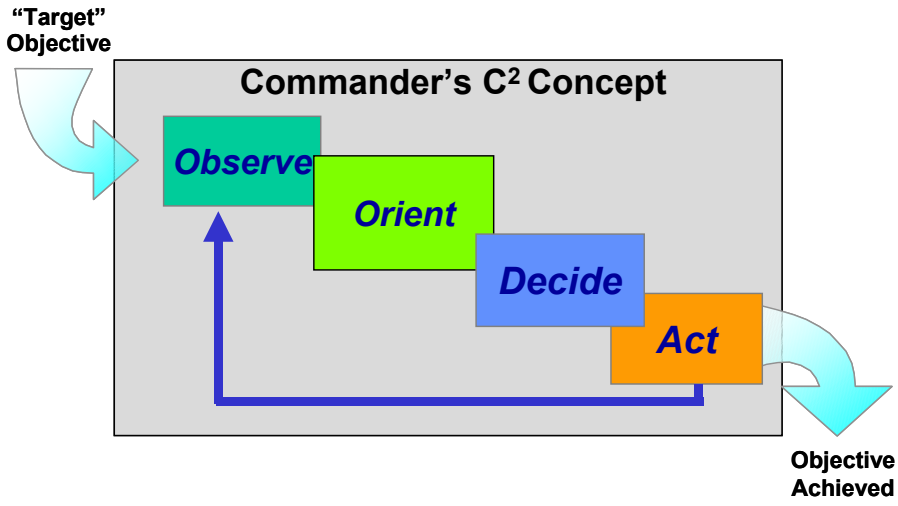

Figure 1. OODA Loop for Command and Control

Today, an "impenetrable" network enterprise (if such a thing existed) would have such limited reach or capabilities as to be of limited usefulness. Network operations and operators have limited insight into the operations of the enterprise (limited monitoring, state explosion for digital systems and networks). Information can be taken (copied and possibly changed without authorization and moved out of the system) without evidence of theft because the digital information remains in storage in the information system. Because penetrations may occur and information and applications may become compromised, it is critical to have the capability to record the events when they occur so that you know what happened (noted as early as 1975 by Saltzer and Schroeder [5]). Techniques employed could/should also be the basis for reliable system operation (e.g., fault/error tolerance, fault/error detection, isolation and recovery), network management, and intrusion detection. Rather than relying on patches, workarounds, and the overt creativity of system and network administrators to somehow establish and maintain information flow – via sneaker net if necessary – with the global enterprise of today and tomorrow's Air Force and other military command and control systems, it is time for the status and mission / operational capability of the network and network applications to be made an integral part of command and control processes in the Air Force enterprise. This need for "cyber situational awareness" as part of command and control processes is a natural outgrowth of information operations as defined in AFDD 2-5 [6] and Joint Vision 2020 [7].

Beyond the physical attacks to systems that may arise during combat or military operations other than war (such as extreme weather), computing networks are subjected to a variety of cyber attacks and probes on a regular basis. For any networked computer system, the staff members are warriors who fend off real and significant attacks every day [7]. From a certain perspective, US Air Force and other Department of Defense computer networks may be among the most "routinely attacked" weapons systems in inventory – the sources of these attacks may or may not be from traditional enemy or terrorist forces and may or may not be detected. US military networks operate

across dedicated and/or leased commercial, wired and/or wireless networking assets, and represent one of the largest and most difficult systems to protect in the world.

The US House of Representatives Committee on Government Reform, Subcommitee on Technology, Information Policy Intergovernmental Relations and the Census, annually reviews the computer security policies and management practices of federal departments and agencies [8]. Congressman Putnam in his statement on federal computer security reported in December 2003 that overall, federal government computer security rating, based upon the Federal Information Security Management Act, had improved from 2002 from a failing grade of F to a grade of D [9]. In keeping with the average, the Department of Defense moved from a failing grade in 2002 to a grade of D in 2003. The report also noted that among three federal agencies not submitting separate, independent Inspector General (IG) reports of computer and network security was the Department of Defense. (The lack of an independent assessment of security policies and implementation of those policies implied that the Department of Defense grade is a self-reported score resulting in a grade of "D.") Among factors cited by the House Government Reform Committee as being important to those agencies such as the National Science Foundation and the Nuclear Regulatory Commission "making the grade" (of "A") were: a full inventory of critical information technology assets; identification of critical infrastructure and mission critical systems; and strong procedures for incident identification and reporting [9].

The identification and marshalling of assets (people, equipment, communications and facilities) and procedures for conducting a mission certainly fall within the responsibility of a combatant commander in a military organization. The same should be said for marshalling necessary networking and computer resources including security and defense capabilities. The need and technical basis for a strong information sharing and information systems architecture for command and control systems to support these types capabilities and support for information operations is described in papers such as those by Heath and Woodcock [10] and Curts and Campbell [11].

The identified need for strong incident identification and reporting procedures points directly to the need for forensic capabilities that should also be part of a combatant commander responsible for achieving any operational mission objectives requiring network or computer resources. Since there are very few missions that don't rely on some form of digital information processing, transmission and storage, it would be a rare mission commander and C2 plan that should not also include forensic capabilities as part of the overall mission plan.

The Role of Digital Forensics in Cyber C2 Processes

There is growing recognition that command and control for computer network defense or "cyber command and control" needs to follow a different path than the traditional command and control approach followed in prosecuting time sensitive / time-critical targets in modern warfare [12,13]. The time criticality of computer network attacks, their ability to rapidly propagate throughout a network, the ability to gain access to time-sensitive information without its compromise being apparent shortens the OODA cycle down to times than may be less than a typical human reaction time of 0.1 s.

Cyber situational awareness, knowing the network's operational state and ability to successfully perform its current mission, is one of those necessary, but not-yet- consistently-defined, -measured or –presented, capabilities required for cyber command and control and conducting information operations (*i.e.,* "actions taken to affect adversary information and information systems while defending one's own information and information systems" [3]). For a command and control system, items of interest may include: the configuration, availability and mission criticality of hardware and software assets; the availability of the people who work with and support the network; what applications are available/executing/awaiting execution; available services and quality of those service; network bandwidth, performance, integrity, and reliability; and what portions of the network are under attack and what types of attack. The ability to collect, validate, analyze and interpret the above types of information and craft it into a "cyber operational picture" that can support decisions to take actions and allow the results of actions to be observed all go into the process of creating cyber situational awareness.

However, being able to know the cyber situation certainly sounds familiar to many of the concepts for digital forensic science embodied in the definition developed at the first Digital Forensic Research Workshop in 2001.

> "Digital Forensic Science – The use of scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation, and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal, or helping to anticipate unauthorized actions show to be disruptive to planned operations." [14]

Another aspect of cyber situational awareness is the time-sensitivity of the information and the time-sensitivity of decision cycles in conducting cyber command and control. In many traditional military C2 approaches, an incident or situation report of a time-sensitive event (*e.g.,* sighting of a high-value mobile target) are forwarded up the command chain, "decision-quality information" is developed, actions are recommended, legal reviews may be accomplished, decisions are taken, other executing tasks are de-conflicted, and the time-sensitive event "mission" is prosecuted with follow-up assessment. In a situation where time is of the essence, there are lots of processes to accomplish, leaving our "fighter pilot" at the end of the chain with precious little time for

OODA'ing. If the incident or situation report were for a computer network attack, in the time it takes to *transmit* the required messages up and down the chain of command, with no time for fusion of information, decision making or review, major portions of the C2 network may also be under attack (whether the attack is successful or not). As described in detail by Howes, Mezzino and Sarkesian [13], cyber command and control requires timely responses, defense-in-depth, and the development of strategy and tactics to prevent cyber warfare from becoming a one-sided battle.

Today's information operations are also driven by their own decision cycle loop" the Protect – Detect – Assess – Respond (PDAR) paradigm described in AFDD 2-5, and graphically shown in Figure 2. The infinite PDAR loop has a "stop loss" posture with an emphasis on protecting assets and implementation of security mechanisms and policies, and responding to an adversary – perhaps the one-sided battle described in [13]. Boyd's OODA loop is based on the idea of figuring out what it takes "to win" or successfully accomplish a mission and then exiting the loop. The OODA loop implicitly includes the full context of the engagement and adversary as part of the observation and orientation processes and dictates that time is a critical element of the decision cycle and a determining factor in "winning" or "losing." For cyber command and control operations, the PDAR paradigm has a solid approach based on computer and network security policies, mechanisms, and practices. The OODA loop, however, would appear to have its strong points for application in C2 operations where missions face asymmetric (cyber) and blended threats.

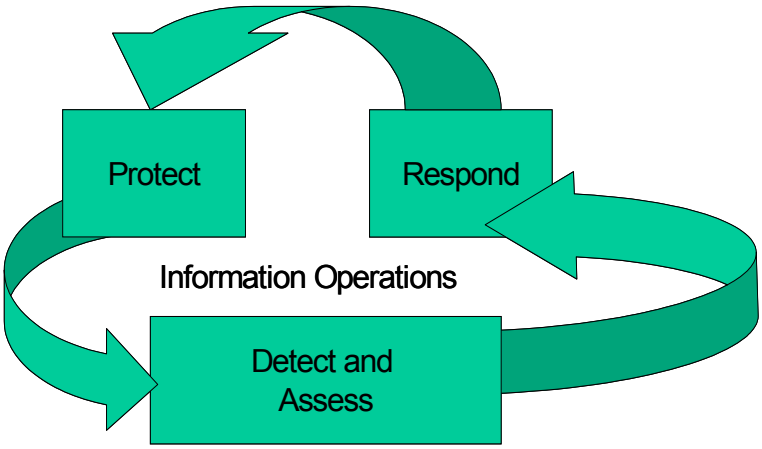

Figure 2. PDAR Loop (as described in AFDD 2-5 [5])

When faced with a cyber or blended threat, commanders and command staffs need to know: what happened, why it happened, what is the source and extent of the event, what are the hallmarks or signatures of the event, and what may happen next. This information is part of building a case for action that is premised upon evidence (*i.e.*, information from observation and orientation) that is common to both forensics and command and control processes. When it comes to being able to make better, *faster* decisions in the global context of military cyber command and control, digital forensics capabilities cannot be

luxuries or afterthoughts. To be effective, digital forensic mechanisms, processes and operations must be an integral and continuous part of observing, orienting, deciding and acting (*i.e.,* the OODA loop) in command and control systems to prevent, detect and respond to cyber events.

Kruse and Heiser describe the basic methodology for digital forensics as consisting of the "three A's": Acquire: Authenticate; and Analyze -- while not altering the original evidence [15]. Laurie [16] adds the additional insight that "good detective work means paying attention before, during and after the attack." Laurie also observes that automated analysis tools are essential and that embedded forensic capabilities must not be a source for potential exploits [16].

Up-front collection of forensic information is an accepted part of other high-value, information-rich systems: such as the "black boxes" in aircraft or the imaging systems in Automated Teller Machines. The black boxes in aircraft are designed to be survivable and tamperproof with the idea that the airframe may suffer an incident or catastrophe during its operation. The black boxes support forensic analyses, are designed to collect and preserve "essential elements" of information, and collected information is designed to provide analyst with situational awareness of the aircraft performance, control surface positions, and flight command crew interactions with the machine system, each other, controllers and communications. The information is not specially developed for forensic purposes but draws from available aircraft information systems. The black boxes do not provide the entire forensic picture for aircraft accident or incident investigations, but they do provide essential elements of information in both determining incident causes and improving design and operation of airframes. Saltzer and Schroeder describe a similar forensic feature, compromise recording, in their 1975 seminal work [4].

The generalized digital forensic science process [14] – also has its own iterative process, but its loop is not necessarily focused on time-sensitive decision making and proceeding even with uncertainty as is often the case in military C2. In structured forensic processes, observations (identification, preservation, and collection processes), lead to an analyst who puts the observations in context (examination and analysis processes) and produces "decision-quality" information (the presentation process) for a acceptance into evidence or a finding or fact (the decision process). Actions in the current paradigm of many digital forensic science processes have tended to be those obtained by legal or judicial proceedings and often represent an end state. This process model serves the law enforcement community well, but may not adequately represent the processes required to make effective command and control decisions in the face of cyber attacks on military networks and critical infrastructure protection systems. Table 1 provides a summary mapping of the digital forensic science process mapped onto both the OODA loop steps and the PDAR loop steps. As Table 1 shows, a clear and distinct mapping across processes does not exist. However, the first three steps of the OODA loop (observe, orient, and decide) do map reasonably well onto the digital forensic science process and indicate that many digital forensic tools and techniques may well find use in cyber command and control processes.

Digital Forensic Science Process	OODA	PDAR
		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

Table 1. Process Comparison Among Digital Forensic Science Process, OODA Loop, and Protect-Detect-Assess-Respond Loop

Opportunities for Implementing Digital Forensics Capabilities in Cyber C2 Systems

As with any command and control process, the implementation of forensics into military command and control processes to improve decision making processes for cybersecurity and cyber command and control operations requires deliberate planning and execution – its own OODA loop – and the arrangement of personnel, equipment, communication, facilities, and procedures as outlined in the following section.

Before discussing what types of forensic capabilities may be implemented in cyber C2 systems, it may be useful to digress for a moment to consider required the digital forensic process attributes for cyber C2 systems. Many of these attributes represent current areas of research or areas for future research. The following bulleted paragraphs briefly describe some key attributes for developing a digital forensic cyber C2 process and corresponding capability.

- Digital forensic cyber C2 processes must capture minimum essential elements of forensic information (*e.g.,* system status, user status, loads, connections, logs, audit logs, unsuccessful and successful attacks) and determine what needs to be collected over what time frames as to be useful for forensic analysis. These are not simple technical issues. Some initial work to examine characteristics of and approaches to developing minimal data sets describing information systems and networks has been supported by the Air Force Research Laboratory (AFRL) and Defence Evaluation Research Agency (DERA) in the United Kingdom [10]. The need to examine readily available system information for forensic exploitation is an area that deserves exploration as has been done by Stallard and Levitt [17].

- Digital forensic cyber C2 processes must be capable of capturing, maintaining, and presenting a "world view" of the cyber C2 system (often called an enterprise) that is being monitoring and subject to forensic analysis (*e.g.,* the embedded weapons platforms, dynamic as units move in and out of areas, resource losses resulting from attrition).
- Digital forensic cyber C2 processes must provide trusted storage of the forensic information (*e.g.,* time stamping, auditing, replication and archival media, compression algorithms, persistence of information storage).
- Because cyber C2 processes must occur across geographically disperse and diverse networks, the processes must have the ability to support remote forensic monitoring, reporting, and analysis. Further the forensic processes and capabilities must not serve as a means for exploiting or attacking the cyber C2 system(s).
- Because rapid responses are required, digital forensic cyber C2 processes must consider fully automated observation, orientation, decision and action processes for controlling resources to carrying out the commander's intent to meet a mission objective. In cyber C2, processes are time sensitivity. If digital forensic processes take longer than the decision cycle allows, they won't be used.

Giordano and Maciag described the unique military requirements and challenges for digital forensics as the following.

"The exploration and application of scientifically proven methods to gather, process, interpret, and utilize digital evidence in order to:

- Provide a conclusive description of all cyber-attack activities for the purpose of complete post-attack enterprise and critical infrastructure information restoration
- Correlate, interpret, and predict adversarial actions and their impact on planned military operations
- Make digital data suitable and persuasive for introduction into a criminal investigative process." [19]

In implementing digital forensics capabilities into cyber C2 systems, the requirements are those of any commander planning to conduct a successful mission. People, equipment, communications, facilities and procedures must be identified and included in the plan.

- People will need to be selected, trained, and made available to work in cyber command and control in operational commands. These people will, most likely need to work in virtual teams with combatant commanders and command staffs, and include non-military members in their cadre. [13]
- The role of humans in the OODA loop for cyber / information operations needs to be critically examined. Human-machine interactions also need to be studied to determine when fully automated forensic processes can and should be used and how humans can interact with time-critical forensic processes. Additionally, cognitive models and behavioral profiles need to be available for forensic use. (Even though digital

forensic science often deals with digital artifacts, 1's and 0's don't attack networks, people do.)

- Solutions must be scalable. Scalability has been an issue with many intrusion detection systems, data mining techniques, and now, potentially, with network forensic data collection and monitoring approaches.
- Cyber awareness needs to be provided as an integral part of situational awareness [13, 18], but providing a suitable representation of the network status "landscape" is problematic and high-level abstractions (*e.g.,* Green/Yellow/Red status indicators) risk becoming meaningless or overly constraining in the face of dynamic operational contexts, even with drill-down capabilities.
- Reliable, remote, distributed network monitoring needs to be provided. System monitoring must have a consistent sense of time, correlate events from widespread sites, recognize and possibly contain ongoing events without alerting the attacker that the attack has been detected and is being assessed and controlled (*e.g.,* misdirection into honeynets and honeypots). Forensic capabilities must continue to operate in the presence of (potentially) compromised hosts and networks.
- Standard, accepted practices and procedures must be developed. Timeline contraction and the massive amount of data requiring analysis in cyber command and control require different approaches than the typical computer forensic analysis of imaging disk drives or other storage media. These practices and procedures must be consistent with any strategy and tactics developed for cyber command and control [13].
- Procedures must be in place prior to their need and continuously and correctly used -- another basic design principle from Saltzer and Schroeder [4]. The availability of forensic analysis capabilities for data collection, and evidence processing also may help to enable capabilities for cyber attack indications and warning.

With these attributes and capabilities in mind, digital forensics should be implemented in cyber command and control systems. A reasonable set of mission objectives for implementing a digital forensics process into a cyber C2 system might be to:

- Make cyber situational awareness with full digital forensic capabilities part of cyber mission planning, execution, and assessment;
- Make digital forensic practice part of standard military cyber C2 operations;
- For information operations, provide sufficient rapid responses to "get inside" an adversary's decision loop

Some Final Thoughts on the OODA Loop and Digital Forensics

One thing that was missing in the digital forensic science process that was present in the OODA loop is the link from decision to action. (To paraphrase Boyd: decisions made without resulting action are taken in vain; and actions taken without decision are reckless.) In establishing digital forensics

capabilities in cyber C2 systems, the potential to establish links between decision-making and actions would naturally exist and allow digital forensics to expand into new capacities and capabilities in such broad areas as planning tools; decision support; wargaming, exercises and experiments; and predictive battle management.

Forensic support for planning activities

- Develop courses of action for missions with significant cyber C2 components Develop hypotheses based upon ideas and intents, drawing upon lessons learned from law enforcement / criminal forensic investigations, rather than any hard digital evidence.
- Analyze alternate courses of action: Course of action tests include the following five areas [20]: adequacy (does the mission have the correct objectives), feasibility (including time criticality), acceptability, variety (if the response is always the same, it become predictable to an adversary) and completeness (are who, what, when, where, how all addressed).

Forensic support for rapid decision-making

- Establish criteria for what constitutes decision-quality information for cyber / information operations (lessons learned from law enforcement and judicial processes would be well served).
- If the assumption is made that the C2 system is always under attack (whether successful or not and whether active or not), then forensic processes should always be active. Cyber attack indications and warning would be a natural outgrowth area for forensics. In this area, the lines between intrusion detection and digital forensics are rapidly blurring.
- Create audit trails for operational readiness inspections and legal reviews

Forensics in wargaming, critical experiments, military exercises

- Build upon C2 experiment at DARPA TIC for Cyber Panel Program with four enclaves [18].
- Build upon the publish-subscribe and intelligent agent based architecture of the Prototype Cyber Warfare C2 System [13].

Forensics processes in predictive battle management

1. Create a network configuration that is an accurate model or representation of an adversary's computer network
2. Simulate a network or computer attack upon the adversary network
3. Identify expected behaviors and observable responses and messages
4. Recognize the effects <u>forensically</u> for "battle damage assessment" or "effects based operations"
5. Use the prediction results
    - Design probes / tests to determine adversary's network configurations
    - Understand the intent of adversary's operations
    - Manipulate the adversary's responses (get inside the OODA loop)

<u>Conclusion</u>

Digital forensic processes and capabilities can play an important role in military cyber command and control. The OODA loop provides an interesting model for adapting the current digital forensic science process to meet the needs of cyber C2 and also provides a guidepost for possible future research and product development directions that will more closely tie forensic capabilities with actions resulting from command and control decisions. However, before digital forensics becomes an integral part of military cyber command and control systems, there are several significant technical issues of its own that must be addressed, including what constitutes minimum essential elements of forensic information for a command and control (or any complex information system), the need to supply forensic analysis continually and in a time-sensitive / time-critical operating environment, and the ability to provide scalable solutions.

References:

[1] Boyd, John R. "A Discourse on Winning and Losing," a collection of unpublished briefings and essays (August 1987).

[2] Sessions, R., Fulcher, S, and Cavnar-Johnson, J., "Planning a Service-Oriented Architecture**," ObjectWatch Newsletter**, No. 46 (February 3, 2004).

[3] Joint Chiefs of Staff, Joint Publication, JP 1-02, **DOD Dictionary of Military and Associated Terms**.

[4] Saltzer, J.H. and Schroeder, M.D., "The Protection of Information in Computer Systems, **Proceedings of the IEEE**, Vol. 63, No. 9, pp. 1278-1308 (1975).

[5] United States Air Force Doctrine Document 2 – 5 (AFDD 2-5), **Information Operations**, 4 January 2002)

[6]Joint Chiefs of Staff, Joint Publication, **Joint Vision 2020** (June 2000).

[7] Whitman, M.E., "Enemy at the Gate: Threats to Information Security," **Communications of the ACM**, Vol. 46, No.8, pp. 91-95, (2003).

[8] House Government Reform Committee, **Fourth Report Card on Computer Security at Federal Deparments and Agencies: Overall Grade D**, downloaded from http://public.ansi.org/ansionline/Documents/ (December 9, 2003)

[9] Putnam, A.H., "Federal Computer Security Report Card" – Statement of Chairman of the House Government Reform Committee, downloaded from http://reform.house.gov/GovReform/News/DocumentPrint.aspx?DocumentID=2025 (December 9, 2003)

[10] Heath, J.E. and Woodcock, A.E.R., "The Challenge of New and Emerging Information Operations," **Command and Control Technology Research Symposium Proceedings**, Newport, RI (2000).

[11] Curts, R.J., and Campbell, D.E., "Command & Control as an Operational Function of Information Warfare in the Context of "Information" – The Nature of Information and Information Transfer," **Command and Control Technology Research Symposium Proceedings**, San Diego, CA, (2004).

[12] Nash, C.L. and Piggott, C.K., " Help! I've been attacked! Researching Ways to Recover a Command and Control System Following an Information Warfare Attack," **Command and Control Technology Research Symposium Proceedings**, Newport, RI, (2000).

[13] Howes, N.R., Mezzino, M., and Sarkesain, J., "On Cyber Warfare Command and Control Systems," **Command and Control Technology Research Symposium Proceedings**, San Diego, CA, (2004).

[14] Palmer, G.W. (editor), DFRWS Technical Report, **A Road Map for Digital Forensic Research**, Report from the First Digital Forensic Research Workshop, August 7-8, 2001, Utica, New York, DTR-T001-01 FINAL (2001).

[15] Kruse, W.G., II, and Heiser, J.G., **Computer Forensics – Incident Response Essentials**, Addison-Wesley (2002).

[16] Laurie, B., "Network Forensics," **ACM Queue**, Vol. 2 No.4, pp. 52-56, (2004).

[17] Stallard, T. and Levitt, K., "Automated Analysis for Digital Forensic Science: Semantic Integrity Checking,"

[18] AFRL Information Directorate, "The Cyber Panel Program," **AFRL Technology Horizons**, pp. 15-16 (September 2003).

[19] Giordano, J. and Maciag, C., "Cyber Forensics: A Military Operations Perspective," **International Journal of Digital Evidence**, Summer 2002, Vol. 1, Issue 2 (2002).

[20] Armed Forces Staff College, AFSC-Pub 1, **The Joint Staff Officer's Guide**, (1997).

---

1. Work supported in part by AFRL Contract F30602-C-03-0063, "Next Generation Spread Spectrum Intrusion Detection Techniques."