Integrated Adaptive Cyberspace Defense: Secure Orchestration

by Keith D. Willett, PhD Candidate at Stevens Institute of Technology, CISSP, ISSAP,

Enterprise Security Architect, National Security Agency Information Assurance Directorate

Abstract

The Department of Defense Strategy for Operating in Cyberspace (DSCOC) calls out the need for active cyber defense (ACD). The function of ACD is to provide sensing, sense-making, decision-making, and acting in cyber-relevant time in order to provide cyberspace defense before an adversary is able to bring about their desired effect. As automation increases and we move ever closer to automated cybersecurity operation, there is an increasing need for automated command and control (C2) to direct the tactical maneuvering of cyberspace assets as well as to provide the logic required to manage this maneuvering. The DoD ACD team is collaborating with the Department of Homeland Security (DHS) Enterprise Automated Security Environment (EASE) activity to define the needs for integrated adaptive cyberspace defense including the needs for agile C2. This paper provides a summary of the DoD/DHS collaboration and describes frameworks, activities, and results to date to define and realize integrated agile cyberspace defense agile command and control as well as a notional definition and description of an ACD *Secure Orchestration* capability.

1 Introduction

The focus of this paper is on integrated adaptive cyberspace defense (IACD) as a capability that describes a functional umbrella encompassing many solutions[1]. This is a vision paper to describe IACD, describe the functional areas of IACD, and elaborate on a *secure orchestration* capability that is part of the IACD mission management functional area. The intent is to socialize these thoughts with interested parties in the United States Government (USG) and industry to establish collaboration in refining the details to ultimately generate requests for information (RFIs) and requests for proposals (RFPs) that will result in operational realization of IACD that includes secure orchestration.

Though not explicitly aligned herein, IACD activities remain aware of and consider the influences from many emerging cyberspace defense and cybersecurity collaboration activities including, but not limited to Enhanced Shared Situational Awareness (ESSA), Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM), Department of Energy (DoE) proof of concept to influence IACD related standards development, and Department of Defense Information Systems Agency (DISA) work to operationalize IACD concepts.

[1] There are differences among a program, a function, and a solution (e.g., tool, product, service). To the Department of Defense (DoD), a *program* is a funding source with finite objectives, schedule, milestones, and deliverables. A *function* is a purpose that may consist of capabilities and activities where a *capability* is an expression of a desired result agnostic of the solution that produces that result and an *activity* is a condition or state in which to achieve a desired end. A *solution* produces a desired result expressed in a capability.

1.1 Active Cyber Defense and Enterprise Automated Security Environment

The Department of Defense (DoD) Strategy for Operating in Cyberspace (DSOC) defines active cyber defense (ACD) as, "The DoD published the Strategy for Operating in Cyberspace in July 2011 with a definition of ACD as the DoD's 'synchronized, real-time capability to discover, detect, analyze, and mitigate threats and vulnerabilities' to defend the department's information networks." (Herring, Willett 2014) The National Security Agency (NSA) Information Assurance Directorate (IAD) is elaborating on ACD as a function. IAD is collaborating with the Department of Homeland Security (DHS) and their activity on Enterprise Automated Security Environment (EASE). ACD and EASE are essentially the same with the only differences being those to reflect respective authorities, where ACD is predominantly for DoD and National Security Systems (NSS) and EASE is predominantly for federal civilian agencies with optional adoption by critical infrastructure and key resources (CIKR). The term *integrated adaptive cyberspace defense* is synonymous with both ACD and EASE, but is neutral in nature by virtue of not being explicitly associated with a DoD, an intelligence community (IC), or a federal civilian agency program. Therefore, any references to IACD are general in nature and apply to both ACD and EASE; reference to ACD is explicitly to IAD's work and reference to EASE is explicitly to DHS' work.

1.2 Active Cyber Defense

ACD is comprised of six functional areas: Sensing, Sense-Making, Decision-Making, Acting, Messaging and Control, and ACD Mission Management (Figure 1). The ACD functional areas (FAs) are essentially observe, orient, decide, and act (OODA) with the addition of coordinate and manage (Figure 1).

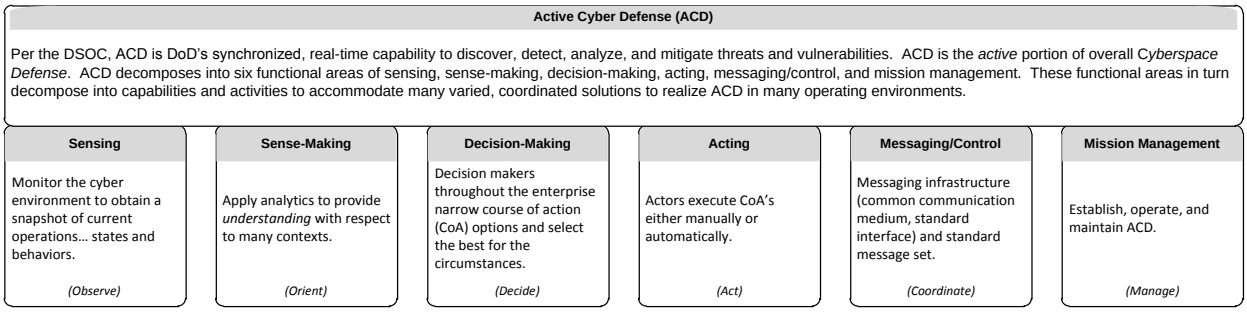

Figure 1: ACD Functional Areas

Fundamental design principles behind IACD are to create a layered and modular design. This implies highly specialized components that perform discreet tasks that take input from other components and provide output to other components. Such a design is ultimately more flexible (i.e., dynamic, adaptable, agile) for discreet refinement, improvement, replacement without the need for broad systemic modifications. As long as the refined, improved, replaced component produces its desired results, IACD overall continues to function effectively. To facilitate a layered and modular design, the *Active Cyber Defense Reference Architecture v1.0* provides context diagrams for each ACD FA. Figure 2 presents the context diagram for ACD Mission Management (MM) where ACD MM includes establish, operate, and maintain ACD. ACD MM currently consists of one capability and five activities. One activity is *Manage ACD Operations* (MM2), which includes the concept of *secure orchestration*. The results of this paper and subsequent critical discussion of the details will influence modifications to the ACD MM FA to

provide greater specificity and clarity in the *ACD Reference Architecture*. There are many more details to ACD MM and to ACD and EASE that are outside the scope of this paper.

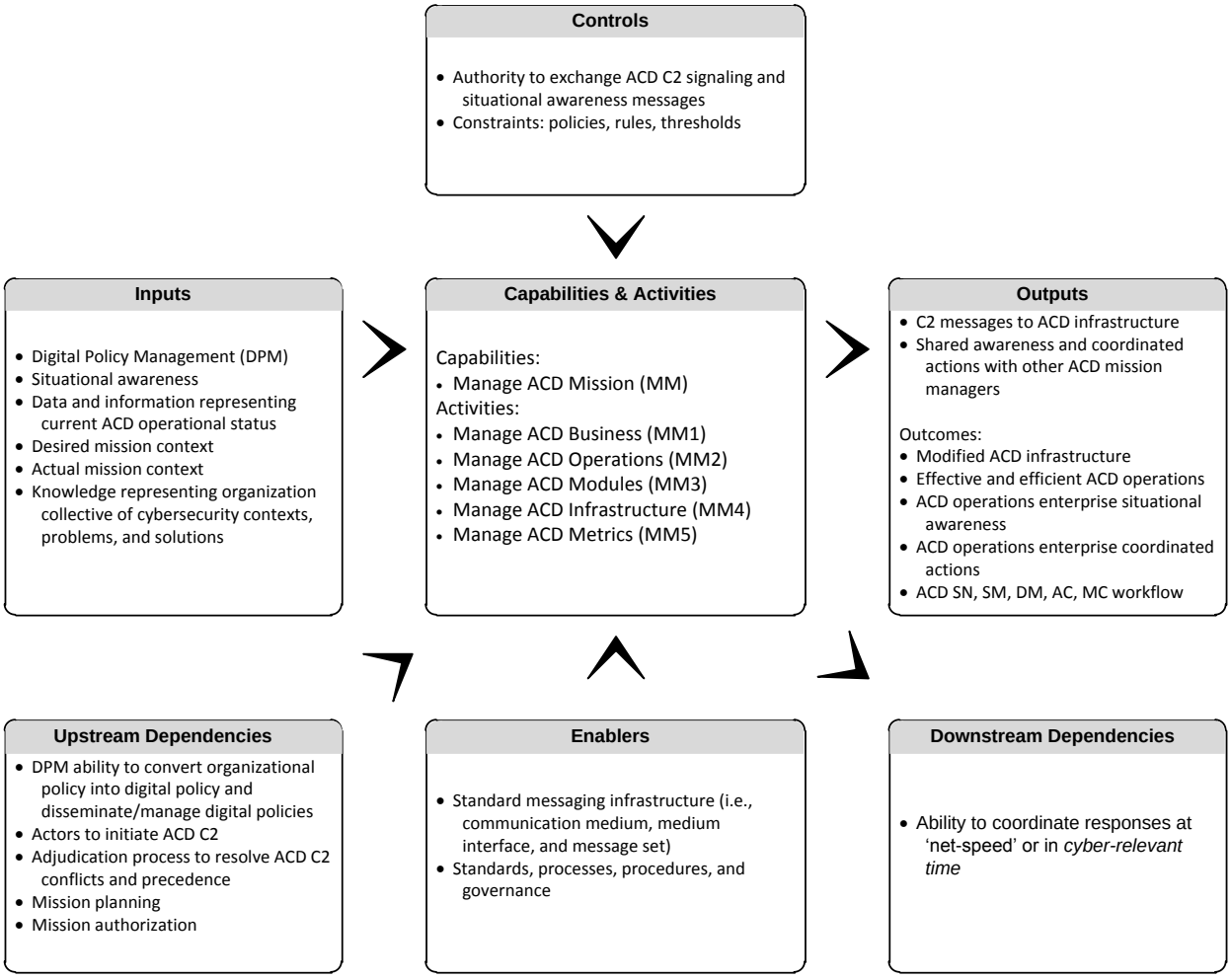

Figure 2: ACD Mission Management Context Diagram

1.3 Enterprise Automated Security Environment

Enterprise Automated Security Environment (EASE) is the DHS program to implement IACD. By explicit design, ACD and EASE align at the enterprise architecture level and enterprise systems engineering level. The only differences are ones reflecting distinct authorities of the DoD and the DHS. The benefits of sustaining alignment between ACD and EASE include the ability to coordinate planning and development, share each other's results throughout the lifecycles of both programs, and plan for the potential of interoperability between ACD and EASE operational capabilities for purposes of *defending the nation* from cybersecurity threats. The following are excerpts from the EASE Request for Information (RFI) on an EASE messaging infrastructure and message set that describe EASE purpose, goals and objectives, desired outcomes, and capabilities.

The EASE concept is an operationalization of capabilities desired for a healthy and resilient cyberspace ecosystem. EASE capabilities are orchestrated to sense and mitigate threats either detected or predicted through traditional and advanced analytic techniques. The goal of EASE is to identify and implement defensive actions to mitigate cyber risks before adversaries can exploit them. This goal is achieved through machine and human-based coordination, collaboration, and analytics in cyber-relevant time[2] at the enterprise, intra-enterprise, and inter-enterprise levels. Standardization across EASE capabilities and supporting infrastructure must use and integrate existing and future technologies.

1.4 Fundamental Drivers – The Why

The fundamental drivers behind IACD include increasing cyberspace operations effectiveness and efficiency. IACD achieves this through the integration, automation, and synchronization of cybersecurity solutions. Secure Orchestration addresses automation and synchronization that includes coordination among people and machines. The synchronization among people largely takes the form of decision support to help people work smarter. People (aka decision-makers) are at every level of the organizational hierarchy including governance, management, operators, and users. Each person makes decisions in some context. Each decision has some decision driver (e.g., legislation, regulation, service level agreement, policy, guidance, etc.). This implies the following requirements to establish fundamental drivers behind IACD operations:

- Enumerate all relevant *decision makers* to which IACD provides decision support
- Enumerate all relevant *key decisions*
- Enumerate all relevant *decision drivers* behind each key decision
- *Decompose* each decision driver into those critical data or information elements necessary to make the decision
- *Translate* the data and information elements into 1) native data elements (i.e., source data), and 2) cyberspace assets containing the native data elements (i.e., native data sources)

The details of these requirements provide the fundamental drivers behind a sensor strategy that includes the types of sensors necessary to collect native data, where to deploy the sensors, and how to configure the sensors in terms of the content to collect and the frequency of collection. This native data then proceeds through a series of aggregation and calculations (analytics) to produce the data/information necessary to provide decision support (Figure 3).

Orchestration involves both people and machine initiated and guided actions. Initially, people will play the predominant role. Overtime, with increased understanding and technical abilities, the orchestration role predominance will shift from people to machine. The role of people will also shift from initially being predominantly *in-the-loop* to being *on-the-loop* where they review and validate the conclusions of machine-encoded logic. IACD will reflect this in a *quality control feedback* capability. This latter activity is critical to maintain accuracy and to maintain a high-level of confidence in the automation appropriately

[2] *Cyber-relevant time* establishes the boundaries for effective cybersecurity actions in the context of a cybersecurity objective. Depending on the context, cyber-relevant time ranges from nanoseconds, microseconds, seconds, and/or minutes.

responding to anomalous activity in the cyberspace environment. Therefore, the *why* driving the introduction and evolution of IACD is to increase operational efficiency via the provision of decision support to people and to shift from predominantly people oriented cybersecurity operations to predominantly cybersecurity automation.

1.4.1 IACD as a Foundation for Cybersecurity Automation

The grand vision for IACD culminates with the realization of cybersecurity automation. Cybersecurity automation has two macro layers: 1) management for making decisions, and 2) mechanistic manipulation for taking action. Mechanistic manipulation consists of the ability to modify the cyberspace environment on-the-fly including the infrastructure, desktops, servers, cybersecurity services and mechanisms, etc. The management layer consists of governance functions that decide (in its literal sense) what to do and adjudication functions that identify problems and decide (in its literal sense) how to resolve them. This vision requires the use of artificial intelligence systems (i.e., expert systems). Realization of such a vision is at least 10 to 15 years away. However, the foundations for realizing such a vision start now with ACD/EASE. Part of that preparation is to lay the foundations for training the AI system in the domain of cybersecurity operations that includes incident response (Figure 3).

Cybersecurity automation imposes machine encoded logic on managing cybersecurity operations. This machine encoded logic requires execution and adaptation according to unfolding circumstances; i.e., the logic must be aware of and consider all the influences on cyberspace operations including threats, assets, vulnerabilities, risk, risk tolerance, security, and mission strategies and tactics. This requires the ability to monitor these areas (observe), understand the current activities and changes in these areas (orient), enumerate and select among available options (decide), and perform some course of action (act). The inputs to cybersecurity automation include data, information, knowledge, understanding, and wisdom (Figure 3). Data takes the forms of native, raw, and refined; and information takes the forms of raw and refined. Native data resides on the data source. Raw data is data collected for a purpose. Refined data is in a normalized format for a particular context. Raw information is a collection of data in human consumable format for a general context; e.g., a report on the United States economy. Refined information is a collection of data in a specific context; e.g., a report on the U.S. economy with focus and its effects on the organization's current fiscal year planning. Knowledge provides a context, a problem, and a solution. Understanding includes relationships; e.g., relationships among knowledge where the whole is more than just the sum of the parts. Wisdom is *the anticipation of consequences*[3] which encompasses predictive analytics.

[3] Norman Cousins

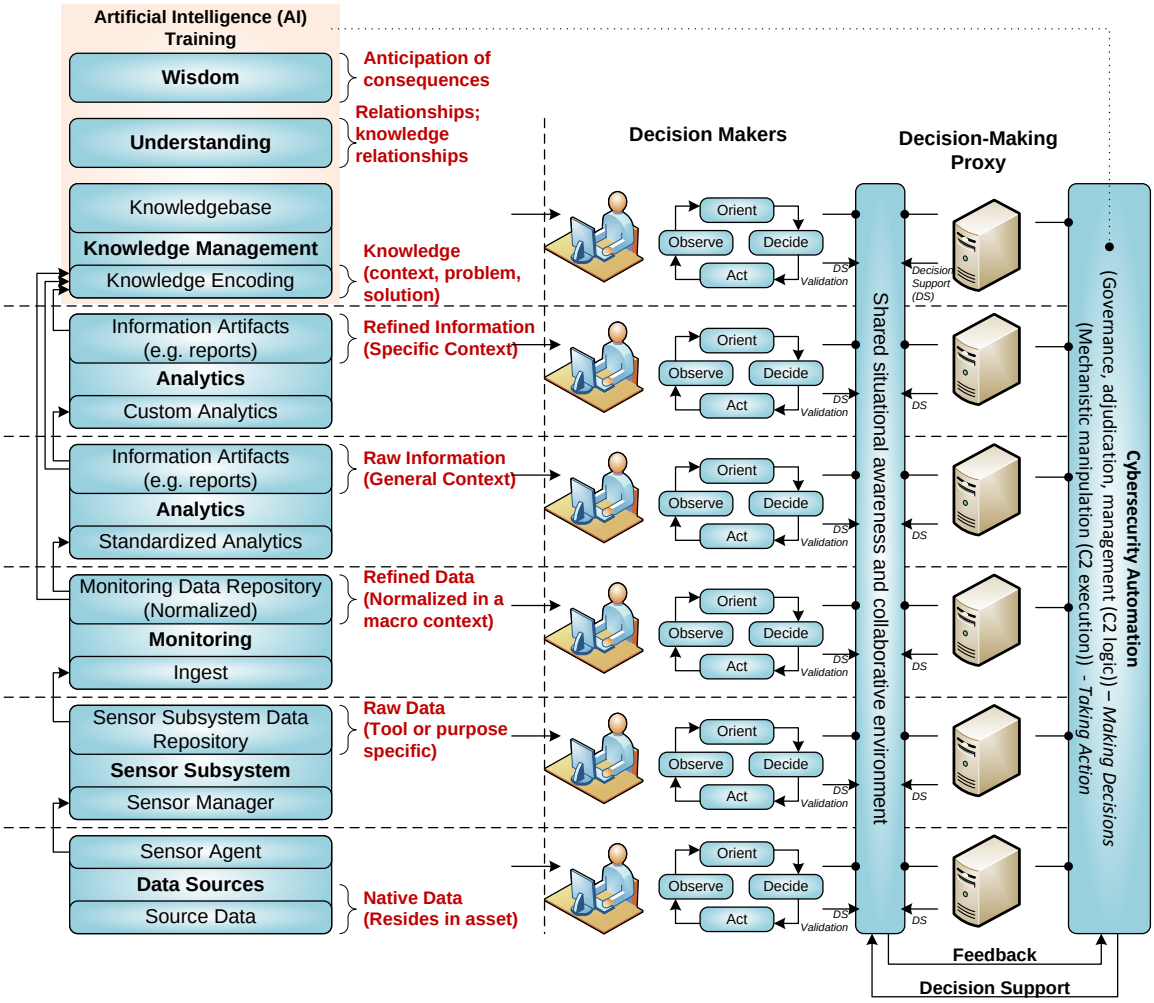

Figure 3: Cybersecurity Automation Perspective

IACD "adaptive knowledge encoding introduces cybersecurity decision patterns (CDPs) and a cybersecurity decision pattern language (CDPL) as formal knowledge representation and a formal knowledge repository to capture, codify, and share knowledge that supports cybersecurity operators and analysts ability to perform timely agile cybersecurity operations. The combination of CDPs and the CDPL provide a cybersecurity cognitive schema that dynamically adapts by assimilating new CDPs in the CDPL structure and acclimating the CDPL structure to new knowledge. CDPs and the CDPL together with applied fundamentals of agile systems engineering help facilitate the design and sustainment agile cybersecurity operations." (Willett 2015) The CDPs and CDPL may also provide a foundation with which to train artificial intelligent systems (e.g., IBM Watson) in the domain of cybersecurity operations. This is part of the path from predominantly people driven orchestration to predominantly machine driven orchestration. There remains the ongoing need to engage people to validate correct decisions and maintain the domain training of the AI system; i.e., people on-the-loop.

2 Secure Orchestration

The IACD mission management functional area includes the establishment, operations, and management of the other IACD functional areas. The operations part of IACD mission management includes facilitating IACD workflow through sensing, sense-making, decision-making, and acting by providing the logic behind the messaging and control of the cyberspace products that provides for automated IACD.

IACD orchestration is the arranging and directing of the ACD workflow to achieve desired operational results. I*ACD secure orchestration* ensures minimal loss or harm to the tactics, techniques, procedures, solutions, and other assets that deliver the desired results from orchestration. At the operational level, "orchestration services involve ensuring correct sequencing of calls to various security control implementations." (APL 2014) IACD secure orchestration provides for functional exchanges among people and machines for purposes of command and control using both synchronous and asynchronous methods.

In less formal terms, orchestration is the logical layer that makes decisions and provides direction to the IACD components that take action to sustain an adequate level of cyberspace operations security. Orchestration is a *workflow-oriented* perspective of IACD operations where influences on workflow include both tactical and strategic considerations. Tactical considerations include keeping a particular server up and operating. Strategic considerations include allowing a particular server to fail in deference to a counterintelligence need to not tip an adversary of awareness of their presence.

Contrary to a workflow-oriented perspective, the sensing, sense-making, decision-making, and acting functional areas maintain a *mission-oriented* perspective. For example, Federal Information Security Act of 2002 (FISMA) compliance is one mission-oriented perspective. Sensors will collect data, analytics will refine the data, decisions will select among viable options, and then perform courses of actions all in context of FISMA. Orchestration does not contain specifics related to FISMA. Rather, orchestration is FISMA aware and will guide the IACD FISMA related workflow in harmony with many other missions. For example, if temporary FISMA non-compliance is required for the success of a higher priority mission, this decision is made by the orchestration function. Such separation of *mission-oriented* and *workflow-oriented* is in keeping the layered and modular design principles of IACD.

2.1 Secure Orchestration Capabilities and Activities

The highest-level capability that encompasses secure orchestration is manage IACD mission (Figure 2). Complementary capabilities for secure orchestration include digital policy management (DPM) with others yet to be determined. To date, DPM has been considered something that provides input to IACD, but external to IACD. Current thinking on constituent capabilities under DPM include Process Input Messages, Maintain Policy, Convert Policy, Validate Policy, Designate Authoritative Source Location, Maintain Authorities, Protect Data at Rest, Publish Information, and Process Output Messages. Note that messaging infrastructure and message set are part of the IACD messaging and control functional area. The IACD layered and modular design distinguishes between the mechanics of tactical execution and the management logic that drives tactical execution.

The inputs to secure orchestration are that which it obtains in order to produce the desired outputs. Secure orchestration is the management logic that provides governance and adjudication for IACD operations. This implies inputs that include the spectrum of what are collectively referred to as compliance requirements, where these include externally imposed requirements (e.g., legislation, regulation), negotiated requirements (e.g., contracts, service level agreements), and internally imposed requirements (e.g., policy, standards). This implies the need for an enumerated list of compliance requirement sources and decomposing these sources into compliance requirements and decision points on what constitutes an adequate level of compliance. Every decision driver is a potential input to secure orchestration and includes strategic, macro-level context (e.g., USG strategy, DoD strategy) and tactical, local-level context (e.g., optimize local performance, local security requirements). The ability to process and resolve strategic decisions and tactical decisions is at first predominantly people-oriented. Over time there will be an increase in automation that includes DPM functions of decomposing organizational policy, deconfliction, and codification in terms of digital policy, plus the application of machine encoded logic for cybersecurity management automation.

The key output from secure orchestration is command and control of IACD workflow via standard message set (yet to be defined) and traversing a standard messaging infrastructure (yet to be defined) that consists of a common communication medium and standard interface such that all constituent solutions of ACD/EASE may interoperate via secure orchestration C2.

The transition processes receive inputs and generate outputs as described above. The execution of the secure orchestration transition processes will include both people and machines. The ultimate goal is the application of artificial intelligence (AI) (e.g. IBM Watson) to perform the governance and adjudication that includes strategic and tactical considerations as inputs to the overall analytic process that produces a list of viable options, selects the optimal option(s) for the current circumstances, and executes the courses of action associated with the selected option(s). The accuracy of such automation requires initial and ongoing training of AI in the domain of cybersecurity automation. The accuracy of such automation also requires the capturing of good decisions and corrective actions via detecting bad decisions, which requires people on-the-loop to validate the automated decisions in adaptable structures (e.g., Bayesian Belief Networks (BBNs)).

3 IACD Operations

In essence, IACD provides adaptive, dynamic, and agile observe, orient, decide, and act (OODA) with the addition of coordination and management of those assets that comprise IACD. Observation (sensing) takes place via sensors that continually take snapshots of current operational states of cyberspace assets. Orientation (sense-making) compares the snapshots of current operations against expected states to determine gaps and their tactical and strategic implications. The decision process (decision-making) identifies viable options on how to address the gaps and selects the best course(s) of action among those viable options. Actions perform the sequence of events that carry out the selected course(s) of action. Coordination uses a message infrastructure and message set to carry command and control direction throughout the IACD infrastructure to perform all aspects of sensing, sense-making,

decision-making, and acting. Management provides the logic that directs the messages. All of this occurs by way of functional exchanges.

3.1 Functional Exchanges

During workflow, there are many functional exchanges to facilitate progress and achieve desired results. These functional exchanges consist of the following:

Who/What Exchanges:

- People to people
- People to machine / machine to people
- Machine to machine

What to Exchange:

- Data:
  - Content, C2 messages (predominantly machine consumable)
- Information:
  - Content (predominantly people consumable)
- Knowledge:
  - Content (predominantly people consumable… initially)

Why Exchange:

- Awareness exchange
- Content exchange
- Command and control exchange

How to Exchange:

- Synchronous and Asynchronous

There are differences among that which facilitates transport (i.e., messaging infrastructure, message set), that which traverses the transport medium (e.g., messages, content), and the logic that guides the use of the message set to execute workflow and provide governance and adjudication to facilitate effective, efficient, and secure operations. Secure orchestration is the management logic for governance and adjudication to facilitate workflow through IACD.

The workflow through the IACD FAs is linear and may flow using FA-to-FA communication or FA-to-orchestration communication. The design principle here is to witness emergent behavior from operations and reflect such behavior in the IACD design documents. In well known, clearly encoded cases, FA-to-FA communication is acceptable and will expedite workflow (i.e., minimize processing time by not waiting for direction from a central management system). At the least, FA-to-FA communication makes orchestration aware of activities just in case orchestration needs to interrupt or modify the flow according to current circumstances. In ad hoc, less clear cases FA-to-orchestration communication is necessary for orchestration to evaluate circumstances on-the-fly and provide direction accordingly. For

example, certain mission goals and objectives coupled with certain observations may prompt the use of analytic tool A. All other details being the same, a shift in mission objectives may prompt the use of analytic tool B. Encompassing such logic in to FA-centric tools is too much of a burden on the tool and the tool vendors (i.e., such logic increases initial and ongoing costs both in terms of dollars and processing time). Placing such logic in an orchestration capability makes more sense in order to dedicate the FA-centric tools to specialized processing (i.e., keep them simple and fast) and modularizing the logic to a dedicated governance and adjudication function. Given the required adaptive nature of the governance and adjudication logic, this design isolates modifications to one area, namely orchestration instead of requiring modifications throughout the FA-centric tools.

Automating a poorly defined process just facilitates getting to the wrong answer faster; therefore, we must capture and codify good orchestration process first for people and then begin to automate the process as people confirm its effectiveness (ability to produce desired results) and efficiency (ability to produce desired results within specified performance parameters).

3.2 Planning and Achieving Secure Orchestration

No single project, no single organizational entity can adequately define secure orchestration, its constituent parts, their interaction, nor define all the standards and applications necessary for its operational realization on a national level to defend the nation from cyberspace attack. The details herein are to seed thoughts and prompt discussion via collaborative partnerships among various aspects of the USG including, but not limited to, the Department of Defense, the intelligence community, the Department of Homeland Security, the National Institute of Standards and Technology (NIST), academic partners, the national labs, industry practitioners (e.g., critical infrastructure and key resources), and solution developers.

Collaborative activities are emerging among the DoD, DHS, NIST, contractor support (e.g., the Johns Hopkins University Applied Physics Lab), and industry. The collaboration spans the areas of ACD, EASE, cybersecurity automation, and standards; activity includes defining and elaborating on enterprise architecture, enterprise systems engineering, traditional systems engineering, capability-based engineering (CBE), testing and evaluation of products based on CBE, identification of capability gaps, capability development, operational deployment, and ongoing operations and maintenance.

3.2.1 Joint Activity Results

A sample of joint activity results include the following artifacts, which remain works in progress but contain sufficient detail to guide planning, systems engineering, acquisition, development, and operational improvements today:

- ACD Reference Architecture
- ACD Enterprise Systems Engineering Plan
- ACD Functional Requirements Document
- EASE Reference Model
- EASE Reference Architecture

- EASE Enterprise Systems Engineering Plan

The Johns Hopkins Applied Physics Lab (APL) is performing a series of spin activities with regard to IACD operational realization. The first of such activities culminated on 30-September-2014 (a two month activity) with the completion of spin zero that focused on orchestration and initial attempts to automate a finite set of use cases. The results were a resounding success.

The test environment to obtain the empirical results was the APL operational network. On a daily basis, there are approximately 1 billion cyberspace events; i.e., anomalies or deviations from the expected. Via an algorithm, details of which are purposely left vague, there are approximately 1 million events identified for prospective investigation by Tier 1 analysts (.1% of all events). The empirical study shows that the best case for a Tier 1 analyst from awareness to appropriate decision-making is 10 minutes, and the worst case is 11 hours. Spin zero focused on orchestration to automate the sequence of events for a particular use case. The automation process' worst case results for a single event from awareness to appropriate decision-making was 10 minutes, and the best case was 1 second. For the best case scenarios, automation provides a 99.83% reduction in processing time and a 98.48% reduction in processing time for worst case scenarios. The orchestration environment in spin zero could scale to handle 24 to 96 events in parallel. Subsequent automated performance of actions took between 30 and 60 seconds. These are promising results that warrant the identification of further use cases and provide justification to further define and elaborate on secure orchestration in order to safeguard and improve the orchestration process.

The design of orchestration for spin zero is by way of capability-based engineering. Certainly specific vendor products were involved, but any given product was integrated via its ability to produce the desired results as defined by the various capabilities. This implies the ability to substitute alternative products that provide the same results. Such a design provides greater flexibility in reusing existing products and substituting alternative products as desirable in a variety of operating environments.

For the time being, writing custom adapters for each product is necessary to facilitate interoperability via automated orchestration. This is similar to when any new peripheral for a personal computer (PC) required a custom device driver. Eventually, the universal service bus (USB) took over and custom drivers were no longer necessary. The intent of the DHS RFI on messaging is to initiate industry collaboration on a standard messaging infrastructure and standard message set. Eventually, these standards will lead to a standard plug-and-play security environment and displace the need for custom adapters. Meanwhile, custom adapters enable improved operations today.

4 Conclusion and Commentary

The vision for ACD/EASE is the first step on a long path to cybersecurity automation. However, such a grand vision will take at least a decade to realize and the USG needs cybersecurity operational improvements now. Therefore, the vision needs refinement into short-term, mid-term, and long-term visions in order to impact operations today, plan and realize incremental improvements over time while moving toward the long-term vision. The short-term vision includes increasing cyberspace and cybersecurity operational effectiveness, efficiency, and security; providing decision support to increase

the effectiveness and efficiency of cybersecurity personnel; and producing an *ACD Reference Architecture* to guide enterprise systems engineering and traditional systems engineering.

The mid-term vision includes increasing use of automation in cybersecurity operations. People will still be *in-the-loop* with regard to making decisions and executing courses of action. People will start to be *on-the-loop* with regard to verifying and validating the automated sense-making (analytics), decision-making (identification and selection of viable options), and acting (performing courses of action). By virtue of being on-the-loop, people provide validation and correction to automation. The results of validation are captured and used to increase the accuracy of automated processing throughout ACD operations.

The long-term vision is for cybersecurity automation including the application of artificial intelligence to provide increasingly automated governance, adjudication, and orchestration of IACD workflow. Increasingly shift people in the IACD workflow to be less in-the-loop and more on-the-loop. Adversaries are intelligent and will discern automated activity patterns, strengths, and weaknesses. As adversaries adapt, so must cyberspace defenses via AI (e.g., learning systems) as well as people discerning new adversary activity patterns, strengths, and weaknesses and reinforcing the correct automated processing as well as refining the incorrect automated processing. IACD is a first step on a much larger path toward defining and achieving cybersecurity automation.

IACD has many capability gaps including the area of standards to facilitate interoperability among security solutions and to facilitate the use of multiple security solutions that produce the same desired results. The latter is necessary to reuse existing solutions and to substitute alternative or new solutions for existing ones. Data standards that specify normalized data structures and content are necessary to develop and apply standardized analytics that in turn produce results for decision support. DPM standards are necessary to facilitate common methods for organizational policy decomposition, deconfliction, and codification in digital policy format for machine-driven tactical execution of cyberspace and cybersecurity operations. Secure orchestration standards will provide for the logic of cybersecurity governance and adjudication for cybersecurity management automation. Standard messaging will facilitate a plug-and-play cybersecurity operating environment. Other capability gaps will emerge as understanding of IACD matures and is reflected in capability and activity definitions.

For secure orchestration, next steps include socializing and obtaining feedback on the definition and elaboration of the secure orchestration capability and its complementary and constituent capabilities. Next steps for overall IACD include processing and pursuing responses for the DHS RFI for messaging infrastructure and message set; engage industry and appropriate standards body to identify and adopt or adapt current standard(s); or, start developing new standard(s). Continue to elaborate on the IACD functional areas to refine the concepts to an adequate enterprise-architecture level detail in terms of capabilities and activities to provide sufficient guidance for IACD related enterprise systems engineering and traditional systems engineering. Elaborate specifically on the decision support aspects of IACD (and other related cyberspace defense constructs) that include the current and future role of people in-the-loop and on-the-loop of cyberspace defense. A supplemental next step is to refine the definition and elaboration of cybersecurity automation as a guiding vision for IACD short-term and mid-term activities.

References

- ACD Reference Architecture v1.0 (unpublished)
- Fonash, Pete and Schneck, Phyllis, *Cybersecurity: From Months to Milliseconds*, IEEE, January 2015 (publication pending)
- Herring, Michael; Willett, Keith D., The Journal of Information Warfare, Volume 13, Issue 2, April 2014, *Active Cyber Defense: A Vision for Real-Time Cyber Defense*
- United States Department of Defense Strategy for Operating in Cyberspace, Department of Defense, Washington, D.C., United States, 2011
- Johns Hopkins Applied Physics Lab (APL), *Integrated Adaptive Cyber Defense – Technology Assessment Summary for Spin Zero*, October 1, 2014
- Willett, Keith D., *Cybersecurity Automation*, Stevens Institute of Technology Term Paper, May 2014
- Willett, Keith D., International Committee on Systems Engineering (INCOSE) International Symposium (IS2015), *Adaptive Knowledge Encoding for Agile Cybersecurity Operations* (proposed paper, pending acceptance and publication)