NPS-AM-20-003

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Acquisition Cybersecurity Management Framework

October 18, 2019

Dr. Randy William Maule, Research Associate Professor

Graduate School of Operational & Information Sciences

Naval Postgraduate School

Prepared for the Naval Postgraduate School, Monterey, CA 93943.

ACQUISITION RESEARCH PROGRAM
GRADUATE SCHOOL OF DEFENSE MANAGEMENT
NAVAL POSTGRADUATE SCHOOL

The research presented in this report was supported by the Acquisition Research Program of the Graduate School of Defense Management at the Naval Postgraduate School.

To request defense acquisition research, to become a research sponsor, or to print additional copies of reports, please contact the Acquisition Research Program (ARP) via email, arp@nps.edu or at 831-656-3793.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School

Abstract

Legacy information infrastructure has proven insufficient for cybersecurity. The acquisition role may be expanded to support information assurance. A supply chain audit and assessment process within the acquisition department will better support emerging cybersecurity requirements. This project advances technical and workflow models, an assessment framework, and implementation methods to expand the acquisition role to include cybersecurity and information assurance across the systems life cycle—from initial requisition to maintenance and obsolescence. Analysis methods and model-based system engineering techniques successfully employed in naval and joint forces field research for nearly two decades, along with best practices from Silicon Valley high technology industries, were applied in the acquisition cybersecurity management framework. A shift of cybersecurity responsibilities from distributed units into central acquisition departments should significantly lessen the inter- and intra-organizational boundaries that have hindered cybersecurity.

Research Objective: Establish models and methods to support the cybersecurity and information assurance needs of naval forces and provide decision-makers with an evaluation framework and workflow to inform acquisition decisions and better ensure information security.

Research Questions: Will the centralization of cybersecurity and information assurance away from individual units into acquisition departments lessen inter- and intra-organizational boundaries that have historically limited cyber effectiveness? Will the workflow and audit models suffice for acquisition departments to implement security controls across the systems life cycle—from initial acquisition through to obsolescence?

THIS PAGE LEFT INTENTIONALLY BLANK

About the Author

Dr. Randy Maule has been with the Naval Postgraduate School since 2000, serving as naval and joint forces enterprise developer, knowledge manager, and technical analyst in Sea Trial and coalition exercises where he conducted systems test and measurement. His enterprise tool suite and cyber test and measurement architecture operated on ships, in maritime and network operations centers, and in forward-deployed commands for nearly 15 years. He previously spent 10 years in Silicon Valley high technology industries researching intelligent networks and service architecture, and prior to this developing enterprise knowledge systems at a federal supercomputer center.

THIS PAGE LEFT INTENTIONALLY BLANK

NPS-AM-20-003

ACQUISITION RESEARCH PROGRAM SPONSORED REPORT SERIES

Acquisition Cybersecurity Management Framework

October 18, 2019

Dr. Randy William Maule, Research Associate Professor

Graduate School of Operational & Information Sciences

Naval Postgraduate School

THIS PAGE LEFT INTENTIONALLY BLANK

Table of Contents

THIS PAGE LEFT INTENTIONALLY BLANK

Introduction

Current organizational structures have proven insufficient for cyber and information assurance. Acquisition departments may be expanded to help ensure cybersecurity. This research advances the acquisition role to support information assurance throughout the supply chain and across the life cycle of the equipment. This is proposed as an enhancement to current acquisition processes. Model-based system engineering techniques are applied for systems test and measurement and integrated into audit processes within the acquisition workflow. Techniques, procedures, roles, and responsibilities are based on lessons learned in naval and joint forces exercises and best practices in Silicon Valley high technology industries. The proposed supply chain audit and assessment process extends from initial equipment purchase order, through acquisition, to maintenance and life-cycle compliance, to obsolescence and destruction.

THIS PAGE LEFT INTENTIONALLY BLANK

Background

Business, industry, and government collectively struggle with cybersecurity compliance, information assurance, and data security. Resources and processes to support audits, assessment, and reporting are insufficient. While the terminology and architecture are slightly different from industry to government, the problems are similar and can often be traced to the supply chain—from counterfeit and compromised components, to improper/malevolent code, to unsecured systems and insufficient maintenance (Lubold & Volz, 2019; Robertson & Riley, 2018).

Holistic efforts to upgrade to a next-generation infrastructure for information assurance have been problematic (Maule, 2011; Maule & Lewis, 2011b) and the cybersecurity problem is now acute (Baldor, 2019). The acquisition role may be best suited to remedy current shortcomings. This will require significant expansion of that role and resources to support supply chain information assurance.

Addressing cybersecurity assessment as a component of supply chain management will shift audit responsibilities from vendors, program offices, and departments into centralized acquisition roles. This will significantly lessen the inter- and intraorganizational boundaries that have traditionally hindered cybersecurity and information assurance.

The shift of systems verification from vendors and their contractors to independent government auditors will remove bias while increasing the comprehensiveness of the process as auditors are able to look across department boundaries to examine the integration interfaces where systems are most vulnerable. Model-Based System Engineering (MBSE) and supporting analysis methods successfully employed in naval and joint forces field research for technology and cybersecurity evaluation for nearly two decades provide the foundation for the acquisition cybersecurity management framework (ACMF) and supporting analysis workflow.

The process begins with technical models, then procedures and workflows for technical analysis, followed by systems integration assessment. Next, methods and

procedures for in-service audits for cybersecurity and information assurance, systems verification, and data validation are described. Technical models are integrated with audit workflows for comprehensive life-cycle systems assessment to include maintenance and the declaration of software/hardware obsolescence and destruction.

Literature Review

Supply chain modeling and analysis is advanced within the context of complexity science, which assumes both technical and human phenomena that interface to determine system readiness and operational effectiveness. Evidence of complexity in naval systems is evident in:

1. Multilayered communication architecture
2. Multiple organizational structures to produce a capability
3. Organizational boundaries that impact engineering and analysis
4. Adversary capabilities for advanced electronic and multilayered cyberattack.

The methodology advances multidisciplinary research techniques to include evaluation of all variables that we have found to impact the validity of naval systems and data, including cross-organizational technology integration, variance in the RF spectrum, and human influence (Maule, 2017). There is a research history that provides perspective.

Network science studies complex networks to generate predictive models (Tiropanis, Hall, Crowcroft, Contractor, & Tassiulas, 2015). For example, tools that we use in naval technical analysis map data flows between systems over network connections to monitor routing, processes, and data. Supporting each variable are algorithms to assess defined metrics and validate data based on components in the routing, integration, and transformation. Network-centric warfare and information dominance are considered within the vocabulary of network science (National Research Council, 2005). When cybersecurity is layered into the analysis, the number of metrics for measurement expands exponentially.

Complexity science spans computer science, mathematics, and operations research and includes the study of distributed, interactive computing (Du & Ko, 2014). Complexity theory investigates how subcomponents of a system integrate to produce a collective behavior of that system (Ladyman, Lambert, & Wiesner, 2013). Pertinent to naval systems analysis is that complexity can be characterized within the context of equilibrium—as required for high-performance communications in challenged

environments. Absent system synchronization, we do not achieve equilibrium, so data relied upon for decisions may be latent, corrupt, or compromised. A sub-discipline of complexity science, adaptive systems, uses probabilistic measures to quantify complex variables, such as systems readiness and human effectiveness.

Adaptive systems are characterized by the capability to change and learn from experience. Machine learning can be applied to help understand the complexity. We observe adaptive behaviors in naval exercises as we instrument networks to monitor complex data flows across geographic regions. The components of systems interact, with the result of those interactions dependent on dynamic contextual variables. For example, changes are made as sailors and systems adapt to rapidly changing tactical scenarios. Evaluation addresses the dynamic interplay of adaptive, complex variables over time. Failure to address this complexity results in an inability to monitor systems to recognize a performance variance or cyber intrusion, or to adapt the analysis to changes in systems operational context—leading to incorrect data.

Test and measurement of naval systems in live operations has established that the relationship between systems, components, and other systems is nonlinear (Maule, Jensen, & Gallup, 2014). It is not possible to precisely define the inputs such that there is a direct relationship to the outputs. Cause–effect relationships can be determined only within technical, operational, and environmental context. Systems performance tends to exhibit divergent patterns under stress, such as challenged communications, jamming or electronic attack, and of course cyber manipulation.

This leads to the final construct of adaptive complexity, namely, that while it is possible to establish linear relationships in a static architecture, these relationships may no longer be relevant when integrated into dynamic scenarios. Researchers have noted the need for probabilistic algorithms for multiple dimensions of analysis when contexts are dynamic and expanding (McMullen, 2015). Assessment is over time, within the full range of technical, operational, and environmental contexts in which the system will operate (Maule, 2016).

Probabilistic algorithms also fit nicely with artificial intelligence (AI) tools for decision support. In warfare, the presence of dynamic variables, together with the large

number of possible contexts to be assessed in an engagement, necessitate statistical analysis. There is never a single answer. The result is always within context. Probabilistic approaches, together with machine learning and neural networks, can address this complexity to provide a solution for supply chain decision-makers.

The need is acute. Problems with unsecured open architecture and open source products persist (Cooper, 2009; Dorofee, Woody, Alberts, Creel, & Ellison, 2013; Lindqvist & Jonsson, 1998). There are problems when vendors publish system specifications to the Internet, and problems with deployment practices that do not carefully control firmware updates (Camp, Goodman, House, Jack, Ramer, & Stella, 2006; Kern, 2014). There is little protection if purchasing computer chips that have already been compromised (Adee, 2008; Center for Public Integrity, 2014; Dean & Li, 2002; Grow, Tschang, Edwards, & Burnsed, 2008; Johnson, 2011; Rossi, 2012).

Another rationale for a direct connection between the audit process and the acquisition role is so that compromised systems can be immediately destroyed and replaced. Historically, after auditors identify a breach, we can only file a report. These reports are not typically well received, and systems may continue to operate. Through the ACMF, the auditors have a more direct means for remediation.

As needed, events can be reconstructed for detailed cyber analysis. We can use live cyberattacks on components in offline laboratories to validate findings. The analysis can produce quantitative system readiness coefficients, and confidence levels for those coefficients (Maule, 2017).

THIS PAGE LEFT INTENTIONALLY BLANK

Methodology

Adaptive complexity for supply chain cyber analysis is applied as an extension of the Cybersecurity Figure of Merit (CFOM). CFOM is a mathematical framework of weighted qualitative and quantitative metrics that provide an expression of the relative effectiveness of an information technology in terms of the completeness and sufficiency of its cyber security properties throughout its life cycle (SPAWAR, 2015).

The NPS Service Evaluation Architecture (SEA) CFOM implementation is based on assessments conducted in live naval, joint forces, and coalition exercises where the focus was on systems readiness and resiliency in electronic engagements against adversaries that had imposed hostile electronic conditions on blue forces (Maule & Lewis, 2009).

Models, metrics, and analytics are derived from cumulative naval system test results, beginning with Fleet Battle Experiments in 2000. Then, FORCEnet and Joint Forces Command (JFCOM) Sea Trials from 2003–2014 including Trident Warrior, RIMPAC, Valiant Shield, and numerous limited objective experiments with NATO and coalition forces.

Cybersecurity Standards

Next is to address foundations for the ACMF. The Cybersecurity Enhancement Act of 2014 (CEA) updated the role of the National Institute of Standards and Technology (NIST) to include cybersecurity risk frameworks. The NIST *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2018) provides high-level structure. The approach features a Framework Core, Implementation Tiers, and Framework Profiles. This ACMF presents a naval use-case for an Implementation Tier, following the categories established in the Framework Core.

The International Organization for Standardization (ISO) is a global network of national standards bodies that develop and publish International Standards. Members are the foremost standards organizations in their countries. ISO collaborates closely with the International Electrotechnical Commission (IEC) and the Institute for Electrical

and Electronics Engineers (IEEE). Some of the standards are specific to supply chain management, including cybersecurity, quality management, and audits (ISO, n.d.). Standards pertinent to the ACMF include:

- ISO 9000: Quality management systems
- ISO/TS 10303-1307: Industrial automation systems and integration
- ISO 16678: Guidelines to deter counterfeiting and illicit trade
- ISO/TR 17370: Data carriers for supply chain management
- ISO/IEC 20243: Mitigating maliciously tainted and counterfeit products
- ISO/TS 22375: Security and resilience guidelines for complexity assessment
- ISO/IEC 27036: Information security for supplier relationships
- ISO 28000: Supply chain security management systems – Specifications
- ISO 28001: Supply chain security management systems – Assessments
- ISO 28002: Supply chain security management systems – Resilience
- ISO 28003: Supply chain security management systems – Audit and certification
- ISO/IEC/IEEE 41062: Software engineering

Specification Framework

The ACMF and supporting workflows apply the NIST methodology and ISO standards through an extension to the traditional systems life cycle. The extension provides cybersecurity management from initial equipment request through vendor selection, then, across the systems life cycle to include maintenance and obsolescence. The intent is to provide a comprehensive security structure for naval systems from acquisition to destruction (Figure 1). This includes the system support structure and command management, staffing, contracting, and outsourcing. Time requirements along with expertise, budgeting, and comparative analysis are addressed.

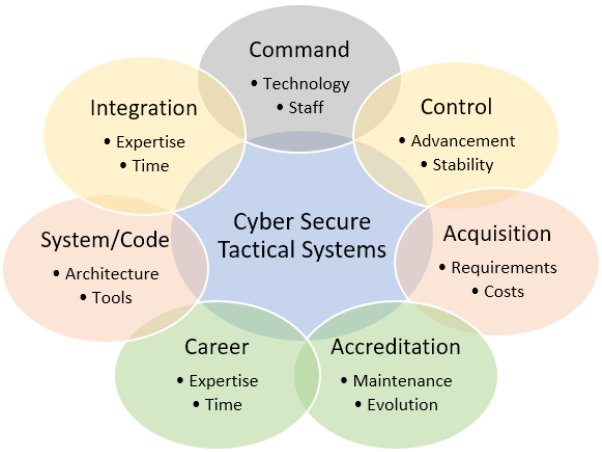


Figure 1. Variables for Supply Chain Cyber Assessment

Evaluation techniques are based in statistical analysis. A deployment of the ACMF would use AI and machine learning to provide decision support. Probabilities are based on defined metrics and measurements from independent government auditors. The method can be applied to help acquisition decision-makers better evaluate technologies for possible cybersecurity impact, and tactical forces to better understand the implications of their purchase requests, the degree to which their systems may have been compromised, and the validity of the data in their systems.

The assumption herein is that when naval architecture is suspected of compromise, and the cyber adversary may have enacted automated routines to alter data to impact systems performance or invalidate information, mechanisms will be required to determine the impact on warfighter readiness. The proposed enhancement to the systems acquisition process will help remedy this situation through real-time audits, monitors, and controls.

Figure 2 denotes the basic acquisition process and the current financial and vendor selection process. Along the left axis is equipment selection and the purchase request. The green arrows indicate legacy operations. Below the basic acquisition process is the proposed cybersecurity enhanced acquisition process. Red arrows denote the additional workflows and data streams.

Within the enhanced process are databases for quality assurance and cybersecurity, along with expert systems to interface with engineers during design and

development, preliminary to product request and submission to the purchasing agents. The green arrows indicate the current workflows, and the red arrows indicate the interfaces to the new systems and processes.

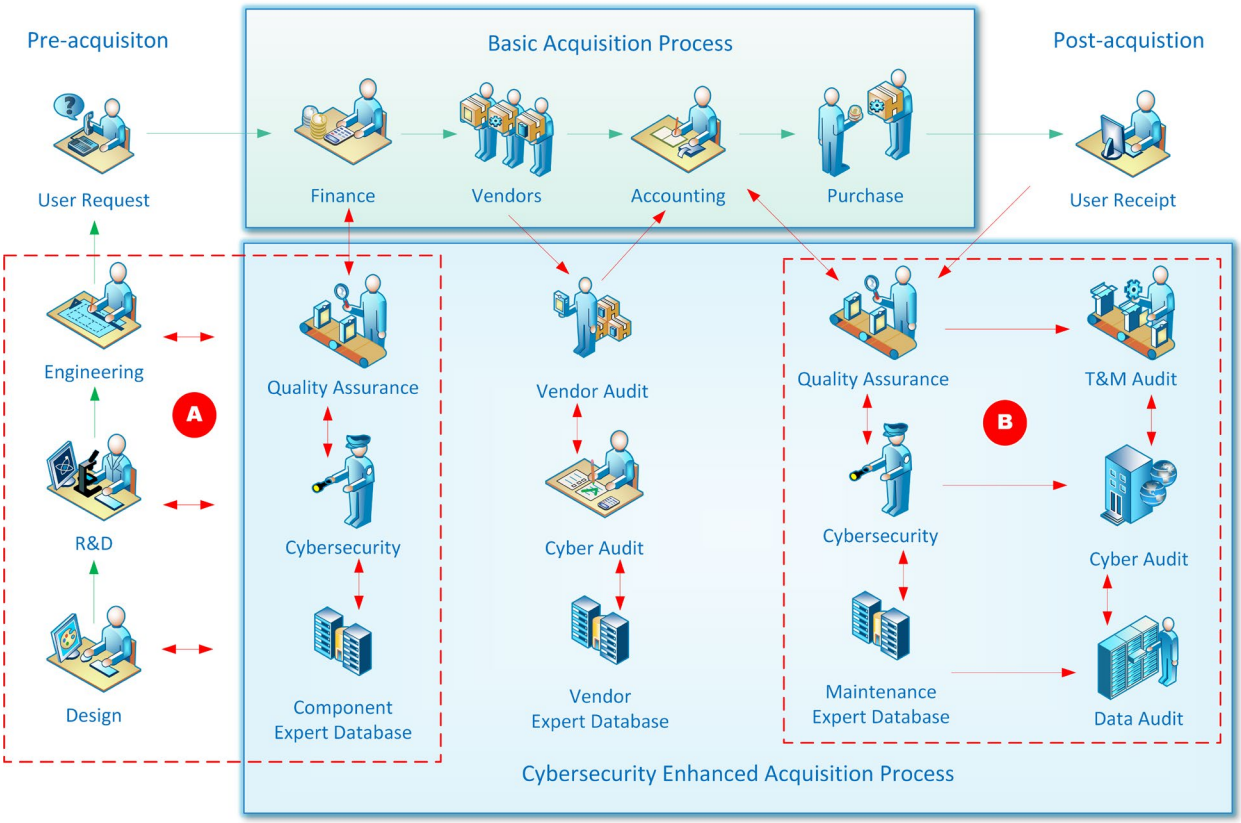


Figure 2. ACMF Information Assurance Workflow

The dashed red box designated as Section “A” is preliminary to the acquisition when the system proponent begins the purchase order. Here the purchaser interacts with expert systems as machine learning agents assess the technology through comparative analysis and provide recommendations. A record stream for acquisition decision-makers and financial personnel is generated. Functions in this area are discussed in the Solution section in this report.

The dashed red box designated as Section “B” is the post-purchase process and consists of a series of independent government monitors and audits. Most can be automated and have been successfully tested in naval operations. These monitors and audits recognize that the purchase is not the end of the acquisition process but rather a

step in the systems life cycle. Before the purchase, the cybersecurity concerns are with the computer chips and embedded components, drivers, and software. After the purchase, the cybersecurity concerns are with the integration, maintenance, and evolution of the software and components within the system, impact on other systems, and the validity of the processed data. Functions in this area are advanced in more detail in the next section and are discussed again in the solution set later in this report.

The unbound area in the middle of the figure addresses the physical components—from the vendor, to the suppliers to the vendor, to the involved personnel. This is a comprehensive area for assessment that is beyond the scope of this project and is reserved for future research. Techniques advanced in Sections “A” and “B” can be applied, albeit with an exponential expansion in detail and complexity.

Maintenance Framework

The audit framework begins with test and measurement models that show components, systems, spectrum, interfaces, sensors, and software. All are assessed within the technical, operational, and environmental context in which they operate to provide a more accurate analysis for acquisition decision-makers. Collected data includes packets, system logs, sensor data, human interface and interaction results, and fusion/integration artifacts (Figure 3).

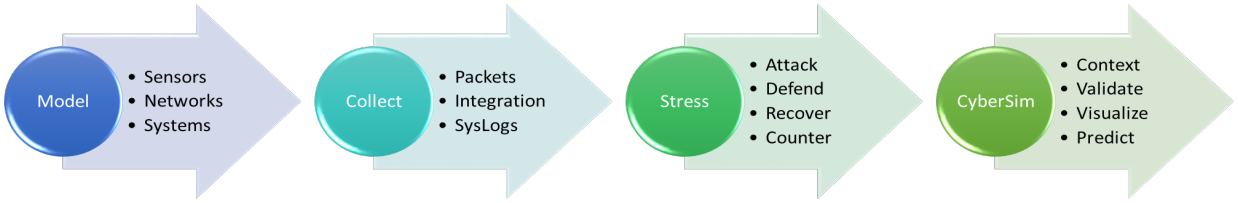


Figure 3. High-Level Supply Chain Cyber Audit Workflow

Analysis of cyber effects begins with stressing systems through network and process load to determine points of failure and countermeasures to achieve resilience. Cyber effects are layered to assess system capabilities to recover from and/or counter cyber stress. Assessment involves a continuous, comprehensive monitoring of systems, networks and applications. CyberSim is for offline tests with live malware against the components to provide a more accurate cybersecurity assessment for systems

verification and data validity. This data feeds the AI routines for algorithmic prediction of systems operational readiness.

In more detail, the ACMF technical analysis (Figure 4) supports in-service test and measurement for continuous systems cybersecurity assessment, using many of the same techniques successfully implemented on forward-deployed ships and in network and maritime operations centers in Sea Trials and coalition exercises. Our audits included not only new innovations but updates to programs of record.

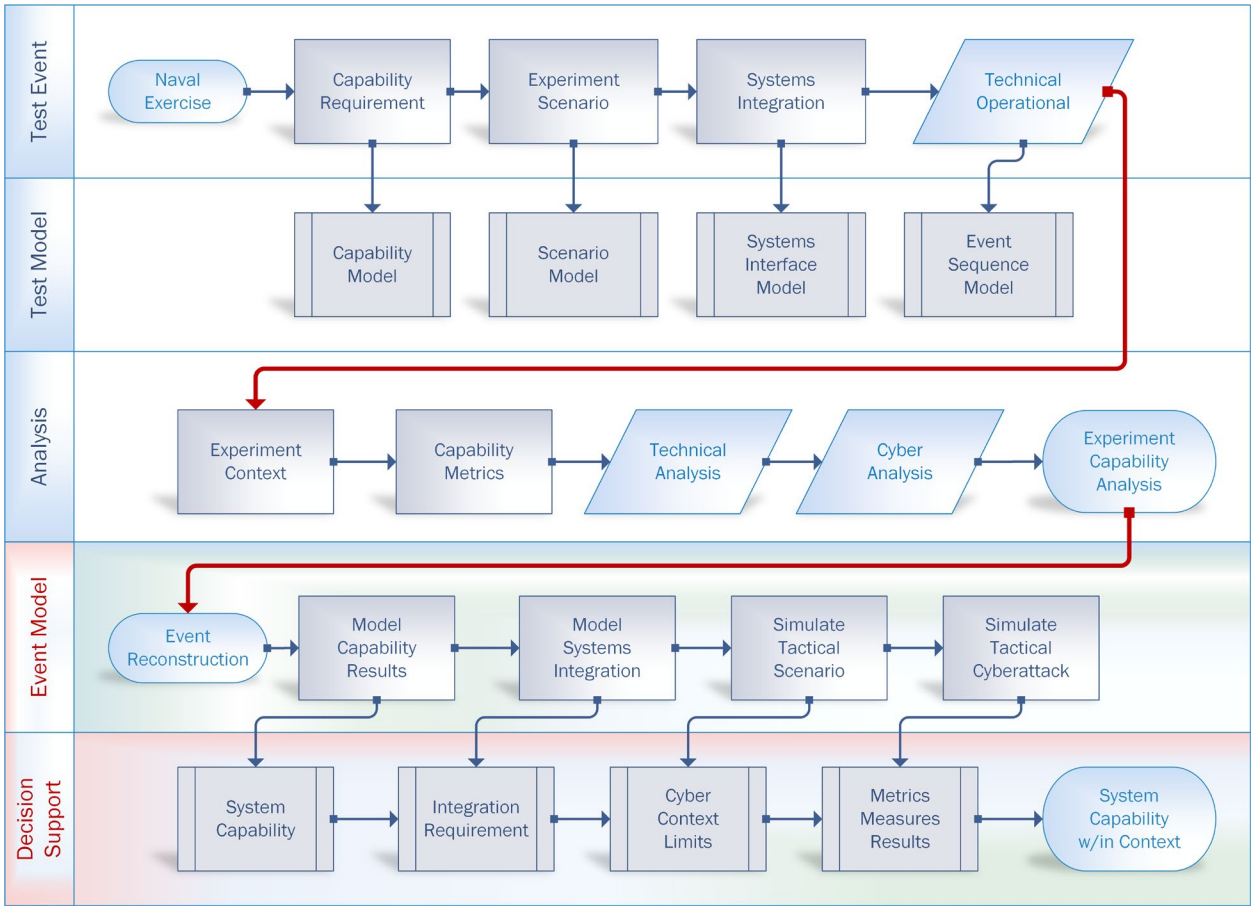


Figure 4. ACMF Technical Analysis Workflow

Cyber analytics is conceptualized as a continuing flow of tests across the operational life cycle of a system. Each operational context, test scenario, vignette, and attack advance the machine learning algorithms and predictive capability of the audit models. In the above example, the analysis is focused on ships in communication-

challenged environments. Systems are under electronic attack—our typical live event scenario in the Sea Trials.

The audit workflow starts with Department of Defense Architecture Framework (DoDAF) models of the system, for which at-rest baselines are established. Systems are then evaluated against these models in at-sea tests with active jamming and cyber/electronic attack. Communications between components/sensors require evaluation of satellite communications, tactical radios, and airborne over-the-horizon capabilities.

Cyberattacks are analyzed for their results on the acquisition component, including system failures, data corruption or manipulation, and degradation of situational awareness of supported command decision systems. Cyber performance and operational measures update or verify models and validate the quality of the data. The process iterates.

THIS PAGE LEFT INTENTIONALLY BLANK

Solution

This section applies the ACMF and supporting workflows as an extension of the systems life cycle to provide structure for naval systems supply chain cyber analysis. Integration DEFinition (IDEF) models represent the operations. Like DoDAF, the IDEF models range from high-level functional models to low-level object-oriented design and simulation (IDEF, n.d.). For a supply chain analytics workflow, the IDEF modeling approach provides useful operational representations in addition to precise data/information metrics for decision support.

The solution set integrates the previous ACMF workflows (pre- and post-acquisition) with implementation constructs for systems verification and data validation to support:

a) Experts and expert systems in the pre-acquisition engineering processes
b) Independent audits for information assurance and systems verification
c) Metrics suitable for machine learning AI support to decision-makers.

Core processes (Figure 5) include IDEF0 inputs, outputs, controls, and mechanisms plus additional audit and AI layers. Core inputs are the purchase order and budget, and outputs are the purchase and supporting maintenance agreements. Controls address guidelines and approvals required for submitters and purchasing agents. Mechanisms include the system, software, or component requirements and specifications.

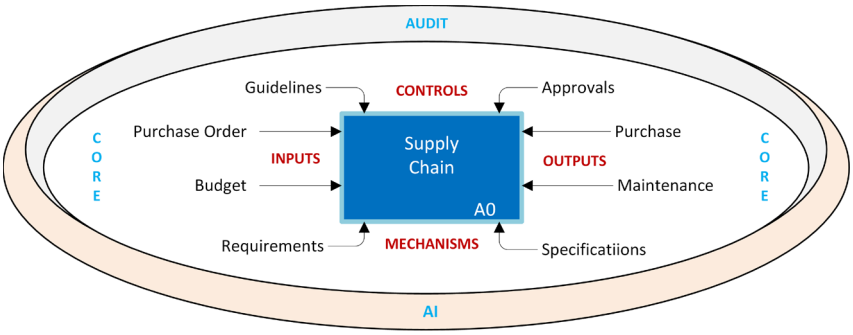


Figure 5. ACMF IDEF A0 High-Level Solution Framework

Cyber Workflow

Figure 6 presents IDEF steps A1–A5 as the high-level components of the supply chain cybersecurity audit workflow. Assessment begins with user requirements and controls to determine whether specifications have adequately addressed technical, operational, and environmental variables that impact the integrity of the equipment in its intended operations.

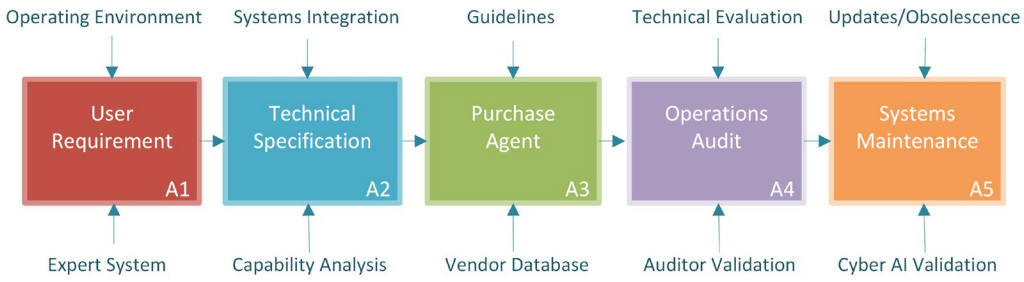


Figure 6. ACMF IDEF A1–A5 for Systems Integrity Analysis

Next are technical specifications with systems integration controls. This becomes a primary data set for machine learning algorithms to address process conflict or operational constraints and will be one of the more extensive programming efforts due to the number of variables in complex, dynamic naval architecture.

In operation, the purchasing agent receives the recommendation from the machine learning output and is simultaneously presented with the option to review the specific criteria upon which the recommendation is based. Controls include restrictions specific to the unit. Upon receipt of the system (hardware, software, service, etc.) the responsibility for verification and validation shifts to the auditor. Upon auditor approval, the system is transferred to the end user.

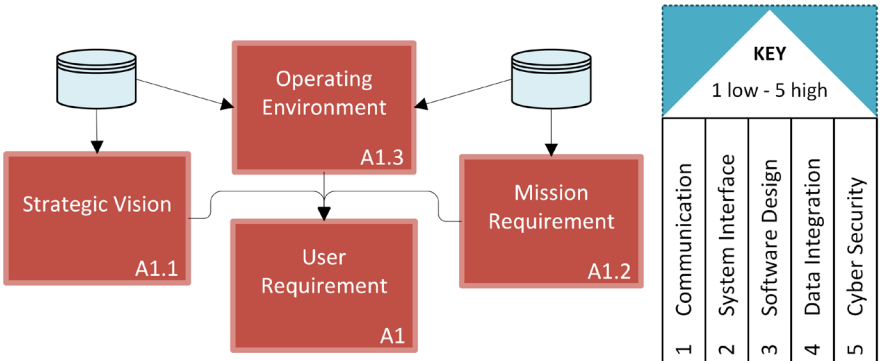
Finally, the maintenance phase monitors equipment throughout its life cycle, including patches and updates until the declaration of obsolescence and verification of destruction. Important is the means to verify that the system or software has been destroyed due to the cyber risk from unsupported components.

Specification Audit

Technical auditors need to be properly trained and equipped with the capability to act independently without fear of reprisal. Nor should they have a vested interest in the success or failure of the system. Technical audits begin during the requirements specification process and initial purchase request (A1 and A2 in Figure 6) and are replicated during the operations and maintenance phases (A4 and A5 in Figure 6).

In "Section A" (Figure 2), the purchaser interacts with the acquisition agent who is supported with an expert system. With enough audits and a supporting database of audit results, the requirements review can be automated such that AI agents provide feedback and recommendations.

Figure 7 models the process and breaks out the Quality of Service (QoS) variables, metrics for those variables, and ratings key. Variables include (1) alignment with the strategic vision, (2) alignment with the mission statement, and (3) alignment with the operating environment. These variables can be programmed into an expert system. The example ratings are notional.



1	User Requirement aligned with Strategic Vision	5	5	4	4	3
2	User Requirement aligned with Mission requirement	5	5	5	5	2
3	User Requirement aligned with operating context	4	3	3	2	1

Figure 7. ACMF IDEF A1 Initial Audit Phase with Variables and Metrics

More difficult are the metrics and rating assignment, which require in-depth understanding of the components of the system and the complexities of the operating environment. A typical approach is to begin analysis with the user's requirements for communication to assess alignment with the vision and mission. Then the specifics of

the operating context, including the organizational, technical, and environmental conditions in which the equipment will operate.

The system interface metric examines integration with the strategic plan and the specific mission area(s) in which the innovation will operate. Context addresses interfaces to technical, operational, and environmental conditions.

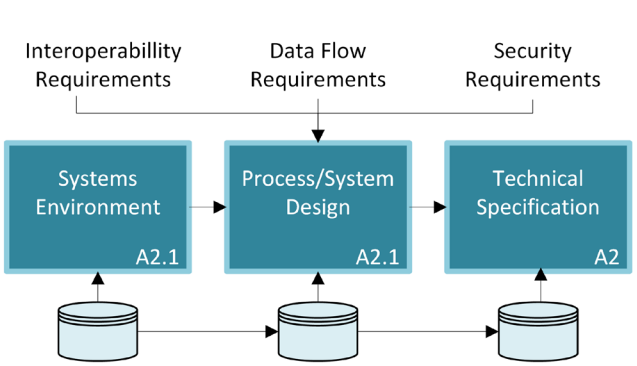
Technical context addresses the specifics of the physical interface—an area for further refinement and additional audit layers in future research. The environmental context categorizes the innovation through physical presence—for example, mobile device versus server, ship versus shore deployment, calm seas versus challenged communications. The operational baseline establishes whether the test is static or dynamic within the specifics of the test scenario. This area will also require deeper analysis in future research.

Software design is more straightforward and looks at the innovation in the context of currently active capabilities. For example, is this a redundant capability? Is the system rated by one of the major laboratories? Is this to be purchased? Developed in-house? Outsourced? In a similar vein, data integration addresses the alignment of the innovation with the vision, mission, and end state: Will data be merged? Will this capability build on the output of another device? Create new insight? Variables are addressed from a command decision perspective.

Placement of cybersecurity in the initial audit helps ensure that information assurance is at the forefront of the supply chain assessment workflow and aligned with the vision, mission, and operating context.

Technical Audit

The A2 technical audit adds detail to the engineering technical measurement process (Figure 8). The workflow addresses specifics within the systems environment, looking at system/service/process integration and interfaces. The first variable assesses alignment of the technical specifications within the designated systems operational environment to establish baselines. Until baselines are established, it may be difficult to discern a performance anomaly or cyber compromise. The ratings are notional.



		KEY 1 low - 5 high				
		1 Systems / Nodes	2 Service Interfaces	3 Interoperability	4 Data Integration	5 Cyber Security
1	Technical specifications address operational environment	5				2
2	Technical specifications address systems environment	4	4			4
3	Technical specifications address system integration	4		3	2	2
4	Technical specifications address data, processes and services	4	4	4	2	4
5	Architecture details operations within context (OV-1)	4				2
6	Architecture details systems interfaces (SV-1)	5	5			2
7	Architecture details systems integration (SV-2)	4		4	2	4
8	Architecture details data and service, process flows (OV-6c)	4	3	3	2	2

Figure 8. ACMF IDEF A2 Technical Specification Variables and Metrics

Performance, interoperability, and integration metrics are assessed for: (a) the technology, (b) the technology within the operating environment, (c) interaction of the technology with the other systems in that environment, and (d) the technology under full operational load from all systems in the environment in a cyber/electronic engagement. Process and data flows are assessed, as is the cybersecurity of the system for each process and data flow.

Systems integration functions are similarly evaluated for performance, interoperability, and integration. This step examines the impact of other systems on the equipment, and the impact of the new equipment on the existing configuration. Data and process flows are examined at the interface level.

The auditors assign weights/ratings to the tests, and these data populate training databases for machine learning. AI helps the decision-makers understand the findings while reducing the complexity of the audit metrics. Future research will complete the process to examine ACMF IDEF models for phases A3–A5.

THIS PAGE LEFT INTENTIONALLY BLANK

Analysis

The analysis method extends traditional structured techniques for communication and systems validation to encompass cyber effects from user activity, for example, forum posts for technical support or chat sessions about user experiences. The desired end-state is automated data discovery using fine-grained metrics for real-time assessment to include all manner of asset usage within the defined operational context. Social media relevant to the use of the technology by the target population may be derived from chat rooms, blogs, forum posts, online reviews, etc.

Important to note is that prior to social networking, the traditional measurement approach of sensor-based sampling was used to characterize technology performance and application usage. Tools to capture services would characterize user processes and security for those processes while monitoring dependencies. Today these measures are insufficient—as evident in the data breaches in the daily news. The supply chain includes not only the initial equipment purchase but vendor selection, installation, interfaces, and most importantly maintenance processes and personnel. Security may be compromised at any phase in the life cycle.

Assessment Process

Figure 9 presents the high-level assessment process. Technical and social analysis is relatively straightforward with qualitative metrics for technology implementation and interfaces, user engagement, and interaction. Measures for quantitative assessment are from system logs, packet capture, and signal analysis. Extension into social and collaborative environments consider user interaction/discussion about the target asset.

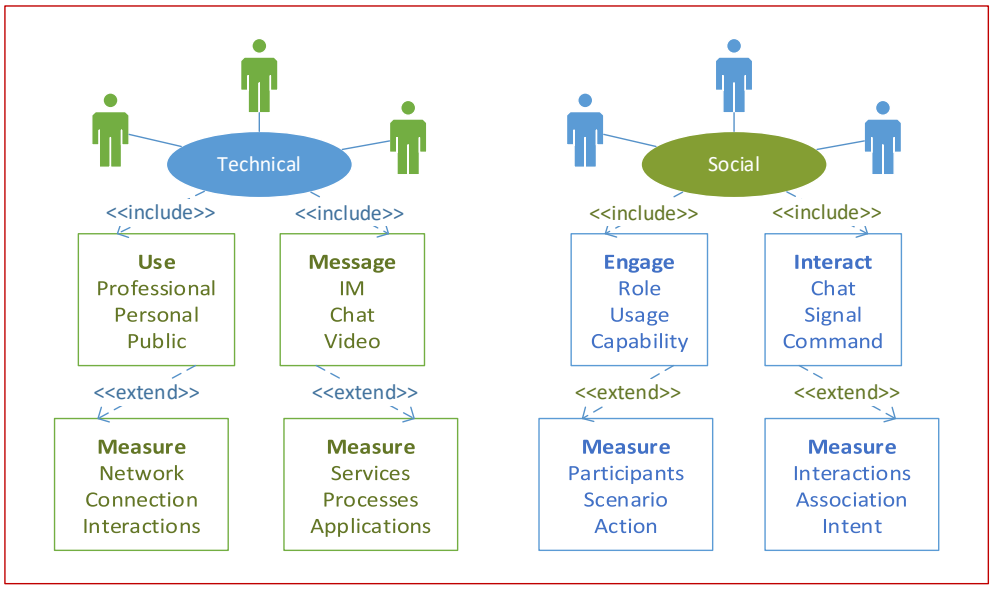


Figure 9. Technical/Quantitative and Social/Qualitative Assessment Variables

Analysis requires event correlation to determine the effects of complex interaction. More complicated are informal signals between knowledgeable participants, for example, notations within a social exchange or group actions around a task or assignment. Measurements would discern the participants, topics, roles of affected users, and actions of users with the system. In this manner complex problems, cyber or otherwise, may be assessed.

At a technical level, conventional packet measurement can monitor participation on a server and application usage within that server. Content assessment of individual participants requires access to application data streams from the server to the client for specific points in time. Analysis requires an understanding of the context of specific media interchanges. Machine learning may be employed to help determine behavior patterns and abnormalities, such as those pertinent to performance problems or a cyber compromise.

While all of this may seem extensive for supply chains, the problem of data manipulation wherein the intent of the attacker is to remain “invisible” requires such comprehensive analysis. Since the breach may occur at any time in the life cycle of the system, supply chain analysis is herein expanded to include life cycle maintenance, system updates, and personnel. Fortunately, most of the analysis can be automated with

machine learning algorithms to establish baselines and identify abnormal behavior. In the case of a sophisticated cyber adversary, the actions can be quite subtle and barely noticeable for even a trained observer.

Traditional technical measurement techniques integrated with social analysis have proven effective in naval exercises for comprehensive assessment of discrete cyber phenomena (Maule, 2017). Interaction analysis is advanced as the means to address complexity problems across the supply chain and over the life cycle of an asset. Measures include media effects in synchronous and asynchronous communications, and data processes in dynamic and multilayered transactions. Figure 10 presents the secondary variables for metric assignment and measurement.

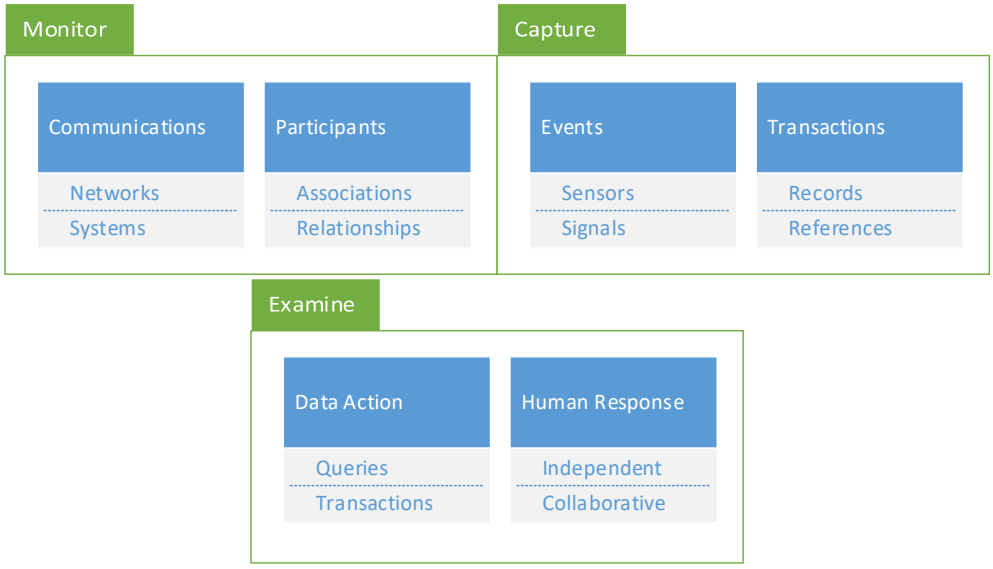


Figure 10. Technical/Quantitative and Social/Qualitative Measurement Metrics

Metrics and measurements help baseline communications within the network environment and radio spectrum. Participant actions can be evaluated for associations and relationships to specific transactions to help assess the state of an asset. Measures become training sets for machine learning.

Events from sensors are captured with metrics for actions and responses. Examples include application queries and user feedback, logs, and media uploads. Human responses include structured actions such as entries into a form, or collaborative actions such as participation in a chat or forum.

Metrics are therein established for systems, applications, participants, and content across all pertinent media channels. The process involves the collection of raw data, the mapping of communication connections, and the assessment of social interaction including chats, instant messages, email, forum posts, and attachments.

To be determined in the requirements and specification phases (pre-acquisition audits) is whether the asset meets the manufacturer's specifications and user requirements. In the implementation and maintenance phases (post-acquisition audits) the performance of the system and supporting systems/networks as well as interfaces for users and support personnel are assessed.

AI and machine learning algorithms can help through compilation and categorization. The very large number of variables can obscure the decision process for supply chain decision-makers who may struggle with the highly complex and detailed findings of technical reports. To help overcome this complexity, the ACMF includes dedicated decision support, specifically, tools with summarization and visualization capabilities for high-level decision-makers needing to quickly understand technical analysis. The intent is to provide a higher level yet equally comprehensive approach to technology, communication, and data analysis for asset assessment across the supply chain and over the life cycle of the asset.

Metrics Research

There is a rich history for analysis metrics. System metrics have been addressed from multiple perspectives. Researchers have separated the physical attributes of communication, computation, memory, and storage from capacity measures such as transaction speed, availability, latency, reliability, and throughput (Zheng, O'Brien, Zhang, & Cai, 2012). Servers, databases and transactions have been stressed to determine availability and responsiveness (Guan, Chiu, & Fu, 2012; Zhao, Liu, & Keung, 2010). Tools selected for the assessment are important.

The Gartner research firm defines *Application Performance Monitoring* (APM) as tracking, in real time, the execution of software algorithms that constitute an application; measuring and reporting on finite hardware and software resources as the algorithms

execute; determining whether the application executes successfully according to requirements; and the recording of latencies associated with execution sequences (Kowall & Cappelli, 2013). We can determine why an application fails to execute successfully, or why resource consumption and latency levels depart from expectations and negatively impact user experiences. Negative readings minimally indicate performance problems, or perhaps malware and data corruption.

To fully understand the complexities of user interaction, the system, its networks, and pertinent applications need to be mapped and transactions profiled. Sensors placed near endpoints and along the communication path can characterize end-state and transmission behaviors. At each level, the supporting analytics must accurately determine operational and behavioral usage to derive baselines and establish patterns. Once the metrics and operational baselines have been established, then researchers can evaluate current measurements against those baselines to assess deviations in system performance and/or user behaviors, which may indicate a breach.

Decomposition of complex or layered services is important. A data repository, social platform, or application may receive data from a remote web service, process and manipulate that data, add new data, and then send the composite including embedded services and links to the end-user. Highly integrated, composite applications and federated web services can be extremely difficult to monitor, decompose, and interpret (Maule & Lewis, 2011a), with data from multi-tenant cloud and distributed systems even more so as traditional security methods may be ineffective (Flood & Keane, 2012; Kalagiakos & Bora, 2012).

Consumption of an input causes a change to system memory meaning that every data or media exchange is significant (Bratus, Darley, Locasto, Patterson, Shapiro, & Shubina, 2014). Differences between a cyber intrusion and normal processes become difficult to discern. Tools can help derive context to trace user access to system resources (Hiray & Ingle, 2013). Frameworks that integrate data collectors, service components, and sensors can help map data interchanges and correlate events for comprehensive system and user analysis (Ficco, Tasquier, & Aversa, 2013; Yassin, Udzir, Muda, Abdullah, & Abdullah, 2012).

Services process data across applications and servers. Process decomposition to assess interactions can help determine risk in services (Parsons, Mos, Trofin, Gschwind, & Murphy, 2008). Metrics include process kills and restarts that impact services, latency within or across services in composite environments, and interfaces between services that govern hardware and user controls. Cumulative or composite services multiply the number of interactions and accentuate analysis complexity (Her, Choi, Oh, & Kim, 2007; Luo, Li, Pershing, Xie, & Chen, 2009).

A traditional technique is to establish metrics for each Open System Interconnection (OSI) model layer to individually assess processes, services, routing, transformation, etc. (Shim, Choue, Kim, & Park, 2008). Then, the coupling and interfaces between the services and clients are assessed (Gao, Wu, Chang, & Meldal, 2006; Kumari, Kandan, & Mishra, 2008; Xiao-Jun, 2009). Analytics focus on deviation from baselines within operational context.

Table 1 assigns these metrics to the previously discussed assessment variables. System logs and packet captures from servers and networks can be processed using traditional techniques and render statistics based on the hosted applications and their services. Measurement is from packet header information, flow data from routers and switches, and agents added to hosts and clients. Agents then summarize and/or visualize data for auditors and decision-makers through a console, portal, or dashboard.

Table 1. ACMF Metrics for Supply Chain Variables

#	Variables	Assets	Metrics
1	Communication Events	Nodes Clusters	*Hardware processes* *Resource links* *Backup, synchronization* *Conflict and resolution* *Archival operations*
2	Communication Sensors	Systems	*Software processes* *Performance under load* *Database performance* *System synchronization, failover* *VM performance and caching* *Authentication/authorization* *Resource contention, resolution*
3	Communication Signals	Networks	*Communication throughput, latency* *Jitter, error identification/correction* *Load, saturation and failover* *Distributed system interaction* *Shared vs. dedicated resources* *Physical and virtual connections* *Agents and system monitors*
4	Transactions Participants	Apps	*Data/component interaction* *Media types and formats* *Usage roles and access* *Interaction/messaging* *Media design* *Throughput and latency* *Distributed component interaction*
5	Transactions Events	Services	*Local user and machine interfaces* *Individual vs. composite processes* *Resource discovery and access* *Remote repository requests* *Remote service integration* *Remote service throughput, latency* *Service monitor capabilities* *Service decomposition measures*
6	Transactions Data Actions	Processes	*Process/component interoperability* *User process de-confliction* *Service process delineation* *Process/resource mapping* *Process reliability measurement* *Object performance parsing* *QoS parameter measures*
7	Data Actions Participants	Security	*Dedicated vs. shared resources* *Transaction flows/dependencies* *Intervention system capabilities* *Monitors for resources and metrics* *Real-time query and processing*

			AI and machine learning variables *Internal/external communication* *High-level resource security* *Low-level data security, validation* *Data replication, synchronization*
8	Data Actions Human Response	Participants	*User authentication/authorization* *Social interfaces* *Collaboration systems* *Communication exchanges* *Peer data integration* *Aggregate/collective interaction*

To note is that sensor agents can be intrusive, adding to latency, reducing working memory, and otherwise detrimentally impacting the user experience upon which it is reporting. Monitor and collection agents can conflict and cause caching and processing problems. Multiple agents along the processing path may conflict and further degrade performance. So, agents can introduce analytic risk—the solution becomes a problem. An assessment is whether the agent is composed of physical devices, a software component, or embedded in a chip or circuit.

Metrics applied for user social interaction are evaluated through the host components, applications, and services. Services supplied to roles or users, processes enacted through those services, and the parameters established for the software, hardware, and communications are measured. Cyber is assessed against these metrics and their operational measurements. There are related metrics for distributed and integrated services. Metrics can be applied for user role or object permissions. To note is that participant interaction must be assessed within the technical, operational, and environmental context to produce a definitive measurement. While the technical metrics are straightforward, there are caches and queues for the objects, which can make analysis challenging.

Decision Tools

With the assessment variables, metrics, and measurement techniques established, the next step is to identify tools to help with the analysis. The approach herein assumes quantitative tools for the monitor and capture, automation to compile the data and render the results, and AI to produce reports and visualizations for

decision-makers. The previously discussed APM tools start the process with high-level analysis of data streams to identify patterns and help discern impact (Craig, 2013).

Network performance tools, end-user experience monitors, and real-time transaction assessment tools help map applications, services, processes, and data dependencies. Some of the tools have predictive analytics (Azoff, 2012) to provide context correlation from packets of identified events (Supasatit, 2012). Sensors capture and appliances filter, replicating and aggregating data to central facilities (Gigamon, 2013) where deep analytics address specific variables of interest (TechTarget, 2017).

Figure 11 provides some examples. On the far left is the previously discussed dependency mapping. This type of visualization is used to illustrate communication, application, process, and data dependencies. In cyber analysis, we look for irregular processes or services. In the middle is a tool we typically use for the measurement of packet flows across servers and applications. This tool will distill fine-grain measurements from data packets in real time for QoS assessment. Deviations are a cause for concern and warrant forensic investigation.

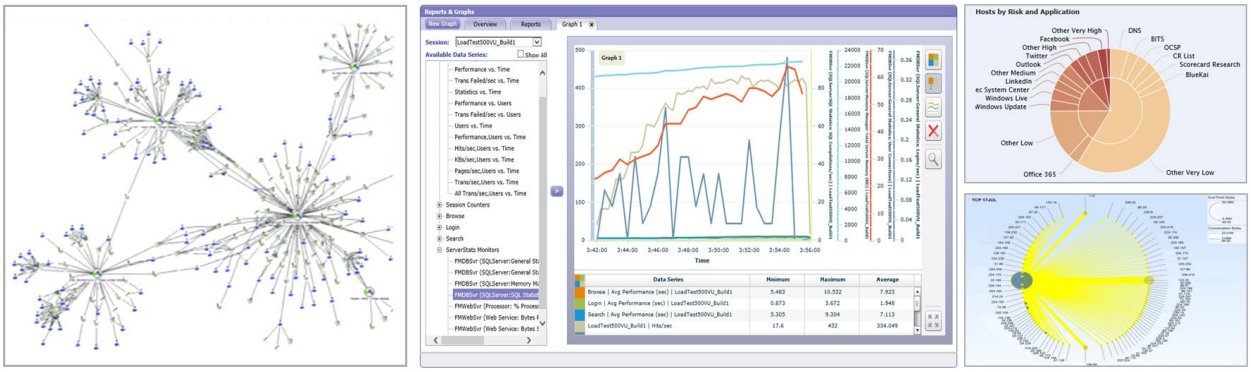


Figure 11. Technical Association and Quantitative Measurement

On the far right are tools we use to visualize data (top) and communication (bottom). From these visualizations the analyst can quickly assess how the equipment and its applications are performing, the degree to which users are active on those applications, and the source and destination for the communications. This is basically a weighted characterization of traffic and communication exchange.

As an example, through the above process and tooling, it was determined that an unexpected communication exchange had been established. This led to forensic analysis for a cybersecurity violation. A compromised chip was identified.

Collectively these tools enable us to parse interactions to determine associations and relationships. Deviations are shown as unknowns. Events can be correlated with algorithms to deconflict processes, eliminate noise, and reduce outlier behaviors (Sani, van Zelst, & van der Aalst, 2018). Weighted connection visualizations help decision-makers understand the degree of association and level of usage.

Data extraction can help determine the nature of suspect transactions. Sensors help determine who is participating or listening. AI can then learn about the interactions to provide recommendations and predictions. Communication patterns can be extrapolated to inform leadership, for example, that a resource is unexpectedly active or that a breach has occurred.

In Figure 12, the analytics engines have correlated the previously discussed technical event information with relevant media usage across collaborative and social applications, in this case, to identify a performance problem with a system and its resources. Specifically, in this tier, we applied cognitive algorithms to assess data patterns and derive behavioral analytics, integrating user, system, and network information. Measures such as “sentiment” are gauged through frequency of words and phrases in chats or forums around the technical events. The correlation algorithms make the connections based on frequency of usage.

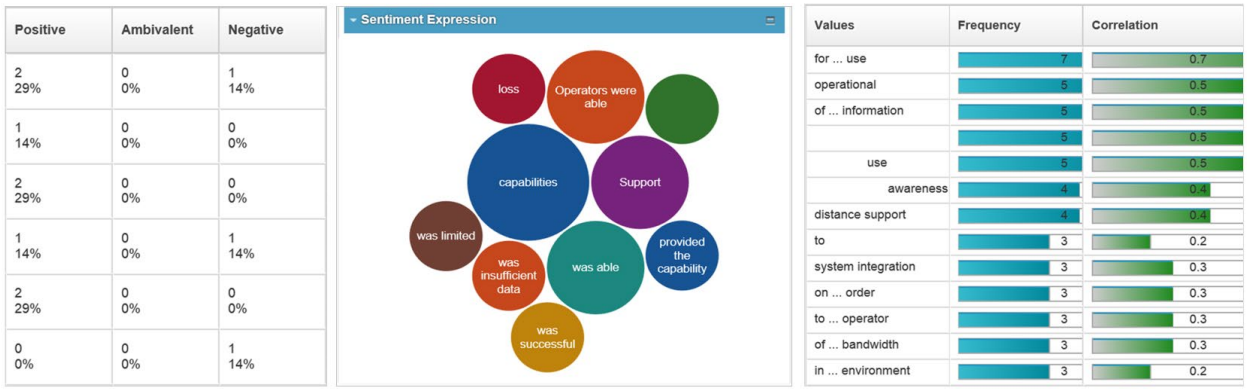


Figure 12. Technical/Quantitative and Social/Qualitative Event Correlation

In the left frame, the system has examined the chat logs around a specific technical event to determine the degree of impact, evidenced by whether the comments are positive, negative, or ambivalent. In the center frame, the social comments around the event have been weighted and visualized as circles so that decision-makers can quickly understand sentiment around the issue and the degree of user discussion around a selected event. The right frame provides the correlation upon which the sentiment was rendered, showing user comments during the event and the frequency of those comments.

In live operations, this technique was used to determine a problem with a mission critical system. The chat logs alerted the analyst who through forensic analysis determined the problem was not with the new system as speculated in the chat logs and support forums but rather with a remote data feed upon which that system depended. The feed was unexpectedly latent from a failure on a remote server. Even more revealing was that the system produced incorrect data when one of its feeds was disrupted and did not inform the operator that a problem had occurred.

Thus, the users had declared a supply chain problem with new equipment when in fact the problem was not with the equipment but a process dependency. More importantly, this holistic approach to supply chain cyber analysis revealed a fundamental flaw in the resiliency of a complex system, which had not been previously known.

THIS PAGE LEFT INTENTIONALLY BLANK

Discussion

This project provided variables, metrics, and methods for supply chain cyber assessment. The technique integrates traditional system and network technical measurement with social media analysis. The process begins with categorization of key variables and the assignment of metrics for systems, applications, data, and services. After the technical measurements, user behavior and informal actions are assessed through social media concerning the equipment in operation.

First, packets are captured for communication assessment, then decomposed for event correlation. Social media is assessed for use of the asset within its operational context. Algorithms support event tracking, analysis of social signals, and correlation with system logs. This provides a holistic analysis of the asset within its technical, operational, and environmental context—all variables that impact the cyber readiness and information assurance of a system.

While this phase of the research does not prevent the acquisition of compromised equipment, it does provide a means to identify compromised equipment prior to deployment and during in-service cyber audits and technical maintenance. Future research may address identification prior to acquisition. Subsequent research may evolve the machine learning and predictive capabilities.

THIS PAGE LEFT INTENTIONALLY BLANK

Conclusion

Supply chain integrity analysis requires assessment of a complex mix of dynamic and adaptive variables. Evaluation includes not only the equipment being tested but the impact of the collective enterprise, the interplay of hosting networks and intervening systems, and remote data processes. Measurements are against metrics derived from models and variables—prior to acquisition for alignment, and post-acquisition for in-service assessment.

Initial levels of analysis were presented, with examples for high-level audit stages with variables, metrics, and measurement techniques. Simultaneously the research addresses the problem of deployment practices, which do not adequately address cybersecurity, information assurance, operational context, and data validity over the lifetime of a system.

This process was active for 15 years on ships, in network operations and data fusion centers, and in deployed shore facilities to assess naval and joint forces technologies. This included field tests of over 500 complex technologies in live operations. Tests integrated quantitative and qualitative functional, performance, and cyber evaluation. Systems integration data was applied for AI and decision support. Through this research, the problems with the supply chain became apparent. Techniques advanced herein were proven to verify systems and validate data.

The process assumes independent audits for quality control, with information assurance and cybersecurity as facets of total quality management. Separation of assessment into an independent unit reporting to acquisition will help avoid entanglements that impacted our field audits and help resolve current cybersecurity and information assurance concerns.

THIS PAGE LEFT INTENTIONALLY BLANK

References

Adee, S. (2008). The hunt for the kill switch: Are chip makers building electronic trapdoors in key military hardware? *IEEE Spectrum*. Retrieved from http://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch

Azoff, M. (2012). *Solution guide: Application performance management*. London, England: Informa UK Limited.

Baldor, R. (2019). U.S. warns of sophisticated cyberattacks from Russia, China. *Fox Business*. Retrieved from https://www.foxbusiness.com/features/us-warns-of-sophisticated-cyberattacks-from-russia-china#

Bratus, S., Darley, T., Locasto, M., Patterson, M., Shapiro, R., & Shubina, A. (2014). Beyond planted bugs in "trusting trust": The input-processing frontier. *IEEE Security & Privacy*, January/February, 83–87.

Camp, L., Goodman, S., House, C., Jack, W., Ramer, R., & Stella, M. (2006). Offshoring risks and exposures. In W. Aspray, F. Mayadas, & M. Vardi (Eds.), *Globalization and offshoring of software* (pp. 182-212). New York, NY: Association for Computing Machinery.

Center for Public Integrity. (2014). Counterfeit chips plague Pentagon weapons systems. Retrieved from https://www.publicintegrity.org/2011/11/07/7323/counterfeit-chips-plague-pentagon-weapons-systems

Cooper, S. (2009). How China steals U.S. military secrets. *Popular Mechanics*. Retrieved from https://www.popularmechanics.com/military/a746/3319656/

Craig, J. (2013). *Application performance management (APM) in the age of hybrid cloud: Ten key findings*. Boulder, CO: Enterprise Management Associates.

Dean, J., & Li, L. (2002). Issues in developing security wrapper technology for COTS software products. *Proceedings of the First International Conference on COTS-Based Software Systems*. New York, NY: Springer.

Dorofee, A., Woody, C., Alberts, C., Creel, R., & Ellison, R. (2013). *A systemic approach for assessing software supply-chain risk*. Washington, DC: U.S. Department of Homeland Security.

Du, D., & Ko, K. (2014). *Theory of computational complexity.* New York, NY: Wiley.

Ficco, M., Tasquier, L., & Aversa, R. (2013). Intrusion detection in cloud computing. In *Proceedings of the IEEE Eighth International Conference on P2P, Parallel, Grid, Cloud and Internet Computing* (pp. 276–283). New York, NY: IEEE Press.

Flood, J., & Keane, A. (2012). A proposed framework for the active detection of security vulnerabilities in multi-tenancy cloud systems. In *Proceedings of the EIDWT Third International Conference on Emerging Intelligent Data and Web Technologies* (pp. 231–235). New York, NY: IEEE Press.

Gao, J., Wu, Y., Chang, L, & Meldal, S. (2006). Measuring component-based systems using a systematic approach and environment. In *Proceedings of the IEEE Second International Workshop on Service-Oriented System Engineering* (pp. 121–129). New York, NY: IEEE Press.

Gigamon. (2013). *Pervasive visibility for the enterprise: Solutions brief*. Milpitas, CA: Gigamon.

Gortney, W., & Haney, C. (2013). *Fleet Commanders' intent: Introduction to the readiness kill chain*. Norfolk, VA: Headquarters, U.S. Fleet Forces Command.

Grow, B., Tschang, C., Edwards, C., & Burnsed, B. (2008, October 10). Dangerous fakes: How counterfeit, defective computer components from China are getting into U.S. warplanes and ships. *Business Week*. Retrieved from https://www.bloomberg.com/news/articles/2008-10-01/dangerous-fakes

Guan, Q., Chiu, C., & Fu, S. (2012). CDA: A cloud dependability analysis framework for characterizing system dependability in cloud computing infrastructures. In *Proceedings of the IEEE 18th Pacific Rim International Symposium on Dependable Computing* (pp. 11–20). New York, NY: IEEE Press.

Her, J., Choi, S., Oh, S., & Kim, S. (2007). A framework for measuring performance in service-oriented architecture. In *Proceedings of the IEEE Third International Conference on Next Generation Web Services Practices* (pp. 55–60). New York, NY: IEEE Press.

Hiray, S., & Ingle, R. (2013). Context-aware middleware in cyber physical cloud. In *Proceedings of the IEEE International Conference on Cloud & Ubiquitous Computing & Emerging Technologies* (pp. 42–47). New York, NY: IEEE Press.

IDEF. (n.d.). IDEF family of methods: A structured approach to enterprise modeling and analysis. Retrieved from http://www.idef.com/

ISO. (n.d.). International Organization for Standardization. Retrieved from https://www.iso.org/standards.html

Johnson, R. (2011, June 27). The Navy bought fake Chinese microchips that could have disarmed U.S. missiles. *Business Insider*. Retrieved from http://www.businessinsider.com/navy-chinese-microchips-weapons-could-have-been-shut-off-2011-6

Kalagiakos, P., & Bora, M. (2012). Cloud security tactics: Virtualization and the VMM. In *Proceedings of the AICT 6th International Conference on Application of*

Information and Communication Technologies (pp. 1–6). New York, NY: IEEE Press.

Kern, C. (2014). Securing the tangled web: Preventing script injection vulnerabilities through software design. *Communications of the ACM*, September 2014, 38–47.

Kowall, J., & Cappelli, W. (2013). *Magic quadrant for application performance monitoring*. Stamford, CT: Gartner Research.

Kumari, G., Kandan, B., & Mishra, A. (2008). Experience sharing on SOA based heterogeneous systems integration. In *Proceedings of the IEEE Congress on Services* (pp. 1–8). New York, NY: IEEE Press.

Ladyman, J., Lambert, J., & Wiesner, K. (2013). What is a complex system? *European Journal for Philosophy of Science,* 3, 33–67.

Lindqvist, U., & Jonsson, E. (1998). A map of security risk associated with using COTS. *IEEE Computer*, *31*(6), 60–66.

Lubold, G., & Volz, D. (2019, September 26). U.S. Navy to appoint cyber chief following a blistering audit: New position is part of broader effort to end plague of cyberattacks. *Wall Street Journal*. Retrieved from https://www.wsj.com/articles/u-s-navy-to-appoint-cyber-chief-following-a-blistering-audit-11569503559?fbclid=IwAR2a74Av_VvRShWI4dl-JG9tAp

Luo, J., Li, Y., Pershing, J., Xie, L., & Chen, Y. (2009). A methodology for analyzing availability weak points in SOA deployment frameworks. *IEEE Transactions on Network and Service Management*, *6*(1), 31–44.

Maule, R. (2011). *Secure Distributed SOA.* Washington, DC: Department of Navy, OPNAV N81.

Maule, R. (2016). Complex quality of service lifecycle assessment methodology. *Proceedings of the 5th International Conference on Big Data*. San Francisco, CA: IEEE.

Maule, R. (2017). *SEA Cyber Figure of Merit (CFOM): Tactical systems cybersecurity assessment*. Monterey, CA: Naval Postgraduate School.

Maule, R., Jensen, J., & Gallup, S. (2014). *Trident Warrior analysis reports 2011–2013.* Norfolk, VA: U.S. Fleet Forces Command.

Maule, R., & Lewis, W. (2011a). Performance and QoS in service-based systems. *Proceedings of the World Congress on Services Computing*. Washington, DC: IEEE.

Maule, R., & Lewis, W. (2011b). Security for distributed SOA at the tactical edge. *Proceedings of the Military Communications Conference.* San Jose, CA: IEEE/AFCEA.

Maule, R., & Lewis, B. (2009). *SOA baseline architecture assessment*. Washington, DC: Department of Navy, OPNAV N6.

McMullen, T. (2015). It probably works. *Communications of the ACM*, *58*(11), 50–54.

National Institute of Standards and Technology (NIST). (2018). *Framework for improving critical infrastructure cybersecurity.* Washington, DC: Author.

National Research Council. (2005). *Network science*. Washington, DC: National Academies Press.

Parsons, T., Mos, A., Trofin, M., Gschwind, T., & Murphy, J. (2008). Extracting interactions in component-based systems. *IEEE Transactions on Software Engineering*, *34*(6), 783–799.

Robertson, J., & Riley, M. (2018, October 4). The big hack: How China used a tiny chip to infiltrate U.S. companies. *Bloomberg News*. Retrieved from https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies

Rossi, B. (2012). Security backdoor found in China-made U.S. military chip. *Information Age*. Retrieved from https://www.information-age.com/security-backdoor-found-in-china-made-us-military-chip-2105468/

Sani, M., van Zelst, S, & van der Aalst, W. (2018). Repairing outlier behaviour in event logs. In W. Abramowicz & A. Paschke (Eds.), *Lecture Notes in Business Information Processing vol. 320*. Champaign, IL: Springer.

Shim, B., Choue, S., Kim, S., & Park, S. (2008). A design quality model for service-oriented architecture. In *Proceedings of the IEEE 15th Asia-Pacific Software Engineering Conference* (pp. 403–410). New York, NY: IEEE Press.

SPAWAR. (2015). *Cybersecurity figure of merit*. San Diego, CA: SPAWAR 58000.

Supasatit, T. (2012). *ExtraHop IT operational intelligence platform*. Seattle, WA: ExtraHop Networks.

TechTarget. (2017). *A guide to Agile testing for QA and test managers*. Newton, MA: TechTarget.

Tiropanis, T., Hall, W., Crowcroft, J., Contractor, N., & Tassiulas, L. (2015). Network science, web science, and Internet science. *Communications of the ACM*, *58*(8), 76–82.

Xiao-Jun, W. (2009). Metrics for evaluating coupling and service granularity in service-oriented architecture. In *Proceedings of the IEEE International Conference on Information Engineering and Computer Science* (pp. 1–4). New York, NY: IEEE Press.

Yassin, W., Udzir, N., Muda, A., Abdullah, A., & Abdullah, M. (2012). *A cloud-based intrusion detection service framework.* In *Proceedings of the International Conference on Cyber Security, Cyber Warfare and Digital Forensics* (pp. 213–218). New York, NY: IEEE Press.

Zhao, L., Liu, A., & Keung, J. (2010). Evaluating cloud platform architecture with the CARE framework. In *Proceedings of the IEEE 17th Asia Pacific Software Engineering Conference* (pp. 60–69). New York, NY: IEEE Press.

Zheng, L., O'Brien, L., Zhang, H., & Cai, R. (2012). On a catalogue of metrics for evaluating commercial cloud services. In *Proceedings of the ACM/IEEE International Conference on Grid Computing* (pp. 164–173). New York, NY: IEEE Press.

Acquisition Research Program
Graduate School of Defense Management
Naval Postgraduate School
555 Dyer Road, Ingersoll Hall
Monterey, CA 93943

www.acquisitionresearch.net