The Post-GIG Era: From Network Security to Mission Assurance

Dr. Kamal Jabbour, ST

ABSTRACT

The shortcomings of the Global Information Grid (GIG) may be traced to a disconnect between cyber policy and technology, and an illusion that cyber defense contributes somehow to mission assurance. Therefore, it is necessary to look past the GIG to a future of affordable access and mission assurance. Prescriptive cyber policies have impeded the mission, as the compliance approach to security led to indiscriminate application of monitor-detect-react constructs to Information Technology (IT) systems regardless of criticality.

In this paper, we present a paradigm shift from cybersecurity through network defense to mission assurance through information assurance. We shift our emphasis from the illusion of building persistent security out of trusted components to the imperative of composing timely assurance out of untrusted components. We distinguish between national security missions and office automation applications and acknowledge the different risk calculus for missile defense versus online commerce. We advocate a shift away from the GIG towards commercial cloud solutions across all phases of the information life cycle, mathematical specification of mission requirements, and implementation validation through operationally realistic testing.

We propose a three-pronged strategy to assure national security missions in a contested cyber environment, focusing separately on legacy systems, current systems, and future systems. Each category brings unique technological challenges, with little commonality within the three categories. We advocate Tactics, Techniques, and Procedures (TTP) wherever applicable, commercial materiel solutions where a TTP-only mitigation falls short, and revolutionary Science and Technology (S&T) where TTP and commercial solutions prove insufficient.

This is a work of the U.S. Government and is not subject to copyright protection in the United States. Foreign copyrights may apply.

Dr. Kamal T. Jabbour, a member of the scientific and technical cadre of senior executives, is senior scientist for Information Assurance, Information Directorate, Air Force Research Laboratory, Rome, New York. He serves as the principal scientific authority and independent researcher in the field of information assurance, including defensive information warfare and offensive information warfare technology. He conceives, plans, and advocates major research and development activities, monitors and guides the quality of scientific and technical resources, and provides expert technical consultation to other Air Force organizations, Department of Defense and government agencies, universities and industry. Dr. Jabbour is an avid distance runner and has completed marathons in all 50 states.

PROBLEM STATEMENT

The myth of intrusion detection dates to the 1980s[1] and has led gradually to a group think culture intent on monitoring networks and computers in the hope of detecting and responding to intrusions in a timely manner.

The introduction of the International Business Machines (IBM) 360 family of computers in the 1960s brought about memory management, dynamic address translation, and resource sharing and, with these advancements, the genesis of time-shared operating systems.[2] In a 1972 USAF report, James Anderson of the Electronic Systems Division at Hanscom Field, MA, singled out resource sharing as a security concern. Anderson dismissed the insertion of security software between an application and the operating system as resource-intensive and ineffective[3].

Two centuries earlier, Scottish philosopher David Hume introduced the induction problem in his 1739 work, “A Treatise of Human Nature”.[4] Hume stated that “there can be no demonstrative arguments to prove that those instances of which we have had no experience resemble those of which we have had experience,” a prophecy of the failure of every cyber defense that relies on the past to secure the future.

The Internet owes a great deal to Robert Kahn and Vint Cerf for developing the TCP/IP protocols[5] on the firm foundation of layering, where Layer N provides services to a higher Layer N+1, and functions at Layer N+1 allow recovery from failures at a lower Layer N. This foundation implies that packet monitoring at the lower Network Layer cannot detect, let alone defeat, cyber-attacks at the higher Application Layer.

Hume, Anderson, and Kahn provide the necessary mathematics to assess the effectiveness of a cyber security tool. If a tool projects the past onto the future, if it requires resource sharing from the system it seeks to defend, or if it operates at the wrong layer, then we assess axiomatically that the tool will fail its intended purpose.

We applied the Hume-Anderson-Kahn axiom to explain the failure of firewalls, cross-domain solutions, guards, intrusion detection systems (IDS), intrusion prevention systems (IPS), virus scanners, malware detection, deep packet inspection, network monitoring, audit logs, blacklisting, white listing, attestation, insider threat detection, normal traffic characterization, abnormal traffic detection, access control lists, honey pots, to name a few. Ironically, a cyber security gadget that violates one of the Hume-Anderson-Kahn laws often violates all three.

BACKGROUND

Layered Architectures

The specification of the Internet Protocol (IP) in the 1970s that we attribute to Robert Kahn and Vint Cerf, and the publication of the International Standards Organization (ISO) Open Systems Interface (OSI) reference architecture, set the stage for a layered implementation of the ARPANET, and subsequently the Internet. At its most fundamental level, the ISO OSI reference architecture specifies that a problem at Layer N can only be fixed at Layer N+1.

The seven layers of the ISO OSI reference architecture map loosely to the five TCP/IP layers:

7. Application Layer	5. Application Layer
6. Presentation Layer	-
5. Session Layer	-
4. Transport Layer	4. Transmission Control Protocol (TCP) Layer
3. Network Layer	3. Internet Protocol (IP) Layer
2. Data Link Layer	2. Media Access Control (MAC) Layer
1. Physical Layer	1. Physical Layer

Each of the seven ISO OSI layers seeks to overcome limitations of lower layers while providing services to upper layers:

7. Application Layer: user and process applications

6. Presentation Layer: data presentation, including encryption and compression

5. Session Layer: session management, login/logout, authentication

4. Transport Layer: host-to-host data transport

3. Network Layer: routing and accounting

2. Data Link Layer: packetization, error detection and retransmission, error correction

1. Physical Layer: raw bit stream plus noise and errors

A similar deconstruction shows the seven layers of a computer architecture:

7. **Application Layer:** user and process applications

6. **High-Level Languages Layer:** 1-to-N constructs, compilers, interpreters

5. **Assembly Language Layer:** 1-to-1 mnemonics, macros

4. **Operating System Layer:** input-output, memory management, resource sharing

3. **Machine Language Layer:** architecture

2. **Microprogramming Layer:** firmware, maps architecture onto hardware

1. **Digital Logic Layer:** hardware, gates

In 1972, Anderson recognized that security problems at the Application Layer (Layer 7) from resource sharing at the Operating System Layer (Layer 4) could not be fixed by inserting tools between the two layers. Such tools exerted a significant performance penalty and failed to mitigate against a skilled adversary. In his assessment, Anderson foretold the failure of host-based security systems.

Similarly, any attempt to defend against security threats at the Application Layer by deploying solutions at the Network Layer violates the fundamental premise of layering on which Kahn built TCP/IP and is destined to fail. Thus, deep packet inspection of network traffic for intrusion detection and prevention, as well as filters and firewalls at Layer 3, fail to detect—let alone prevent—covert channels at Layer 7.

Layering introduces a fundamental asymmetry that frustrates security novices seeking the cyber high ground, or the race to the bottom, suggesting that the process that owns Layer 1 controls the environment. This suggestion is partially true: a Byzantine hardware failure at Layer 1 increases the risk of application failure at Layer 7, but well-behaved hardware does not assure application success in the presence of an ill-behaved operating system.

For mission assurance, we interpret this layering asymmetry differently: a cyber-attack that compromises the hardware increases the risk of mission failure, but a secure processor does not assure mission success against attacks on the intermediate layers.

Efficiency versus Effectiveness

Artificial Intelligence (AI), Machine Learning (ML), Big Data (BD), Command and Control (C2), Behavior Modeling (BM), Automation and Autonomy (AA), promise to increase the efficiency of well-behaved processes, but have no impact on the effectiveness of these processes. In other words, applying AI-ML-BD-C2-BM-AA to a signature-base IDS will not improve its ability to detect a zero-day exploit, but rather increases the rate and frequency of IDS failure.

User Training

No discussion of the failure of cyber defense is complete without an honorable mention of the poster child of cyber failures; user training. From inserting thumb drives and clicking on hyperlinks, to opening attachments and phishing emails, the proverbial dumb user has fueled an insatiable appetite to regulate and train. Notwithstanding the effective technology solutions that can reduce the mission risks from dumb users and spare the dumb user the elusive pursuit of cyber expertise, policymakers demand compliance and threaten discipline.

TOOLS AND TECHNIQUES

Risk Metric

The National Institute of Standards and Technology (NIST) defines the risk to information systems as a function of the likelihood that a vulnerability exists; the threat necessary to exploit the vulnerability, and; the effect resulting from a successful exploitation:[6]

$$\textbf{Risk} = \textbf{P}(\text{vulnerability}) \text{ x } \textbf{P}(\text{threat} \mid \text{vulnerability}) \text{ x } \textbf{Effect}$$

We interchangeably use the terms effect, impact, and consequence.

Our vulnerability assessment of various systems led us to define three classes of potential vulnerability:[7]

i. **architecture vulnerability:** resource sharing and Byzantine behavior

ii. **specification vulnerability:** protocols and Modes of Employment (MOE)

iii. **implementation vulnerability:** hardware, software, and configuration.

Unfortunately, current vulnerability scanning tools have the narrow scope of less than 10 percent of the vulnerability surface, as they look primarily at configuration vulnerability. The effectiveness of these tools over that scope is another matter (Hint: zero). Yet these tools increase the risk to these systems by increasing their attack surface.

We break the cyber threat[8] into three components:

i. **capability:** time, talent, and resources necessary to exploit a vulnerability

ii. **access:** physical, network, wireless

iii. **intent:** we assume malicious intent.

The conditional nature of adversaries threatening to exploit a potential vulnerability implies that there is no threat without vulnerability. This is a fundamental concept that shows how ineffective it is to focus narrowly on defeating threats without taking vulnerability into consideration.

We focus on degree and duration as the two aspects of successful exploitation of a vulnerability. We consider disruption to be a temporary and partial affect; denial a temporary but total effect; degradation a permanent but partial effect; and destruction a permanent total effect.

The duration of adverse effects of a cyber-attack is a function of mission duration. When we measure the duration of many critical functions in seconds, a monitor-detect-respond-recover approach operates inevitably in recovering from mission failure.

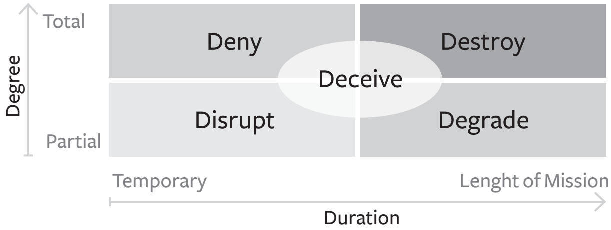

Figure 1. Effects of a cyber-attack

Scope, Effectiveness, and Risk

Prior to mandating a new procedure or implementing a new policy, it is imperative to assess its utility in terms of scope, effectiveness, and risk. Such assessment applies equally to host-based monitoring tools, manned activities, and compliance enforcement.

An assessment of a security artifact begins by defining its scope—the percentage of the attack surface it seeks to cover. For example, deep packet inspection on a network carrying 70 percent encrypted traffic has a scope of 30 percent. Similarly, a Windows vulnerability assessment scan against an aircraft has a scope of zero, and a penetration testing scan against a satellite will fail to detect an architecture vulnerability.

Given the scope of a cybersecurity gadget, measuring its effectiveness allows computing an estimate of its utility as the product of scope times effectiveness. Unfortunately, when a tool violates Hume-Anderson-Kahn, its effectiveness against an advanced threat computes to zero, giving zero utility regardless of breadth of scope.

Compliance enforcement requires selecting security controls deemed applicable to a mission, implementing these controls, then testing these controls. If a chosen security control relies on the past to secure the future in violation of Hume, or if its implementation requires sharing resources with the system under test in violation of Anderson, or if the control operates at the wrong layer in violation of Kahn, then compliance enforcement turns an ineffective compliance vehicle into an attack vector.

Information Assurance Tenets

The three tenets of information assurance are confidentiality, integrity, and availability. The Advanced Persistent Threat (APT) targets information confidentiality by hiding for an extended period of time on a target and copying information. Destructive attacks do not hide; they target information availability by destroying information and computers. Access-less attacks, such as Border Gateway Protocol (BGP) exploits, target information integrity by hijacking traffic and injecting incorrect information.

The most challenging attacks are those that target information integrity. Byzantine fault analysis provides the science to assess system vulnerability to integrity attacks. A Byzantine fault creates the same effect regardless of intentional or accidental cause.[9] In simple words, Byzantine fault analysis looks at the effect when a computer lies, not when a computer dies.

Information Lifecycle

The evolution of military systems from Government Off-The-Shelf (GOTS) to Commercial Off-The-Shelf (COTS), the outsourcing of integrated circuit fabrication and software development, and the transition from dedicated transmission lines to commercially-procured leased circuits, have increased the dependence on a diverse supply chain and a commensurate risk of supply chain manipulation. Besides hardware we did not build, software we did not write, and circuits we did not lay, the shift from GOTS to COTS includes protocols we did not specify, users we did not train properly, and operators we did not educate adequately.

The DoD has neither the will nor the ability to reverse the shift from GOTS to COTS. Therefore, it is unrealistic to expect that the security of the supply chain will improve with new ways to monitor-detect-respond to security failures, leaving us with no choice other than assuring our missions with untrusted components—hardware, software, networks, protocols, users, and operators.

Composing mission assurance with untrusted components necessitates assuring information—the only asset that we own and control—across the six phases of the information lifecycle:[10]

i. Information generation

ii. Information processing

iii. Information transmission

iv. Information storage

v. Information consumption

vi. Information destruction

Disciplined cyber vulnerability mitigation must assure information flows throughout a mission across the entire information lifecycle.

OUR PROPOSED SOLUTION

Vision, Mission, and Strategy

We envision an enduring assurance, a cyberspace with no vulnerability. We seek to assure critical missions through a paradigm shift from computer security to information assurance by creating a cyber domain that assures information across all stages of conflict, leading to friendly missions with no vulnerability in peacetime, denying the impact of cyber threat in escalation, and exploiting at will adversary missions in wartime.

Our strategy uses Byzantine fault analysis to develop dual-purpose Science and Technology (S&T) to create provable mission assurance through disaggregation and composition of untrusted components, and to disproportionately increase the cost to the cyber threat, while holding at risk adversary missions.

The big building blocks of this vision rely on breaking down information risk into its stochastic components of vulnerability, threat, and impact. This breakdown provides threat independence through Byzantine fault analysis. For current and legacy systems, we propose mission assurance through prioritization of Mission Essential Functions (MEF), cyber dependence, vulnerability assessment, and vulnerability mitigation.

Enduring assurance requires designing future missions by mathematical specification and formal verification and implementing information disaggregation and just-in-time mission composition of untrusted components into assured missions with physics-based security. We advocate cyber deterrence[11] through superiority at a time and place of our choosing with intelligent cyber agents that operate on a continuum from direct command-and-control through automation to autonomy. Our vision of enduring assurance requires developing a cyber workforce through education on the science of information assurance and training on the art of cyber warfare and developing a scientifically relevant cyber doctrine[12].

IMPLEMENTATION ROADMAP

Mission assurance of legacy and current systems

MEF cyber dependence requires a disciplined vulnerability assessment of the architecture, specification, and implementation, followed by a systematic vulnerability mitigation through TTP, materiel solutions where available, and S&T in the absence of commercial solutions.

Byzantine fault analysis focuses on information integrity and enables MEF migration into public clouds in virtual machines, direct code translation, or mission revalidation and mathematical synthesis.

We propose the following phased implementation of mission assurance of legacy and current systems:

i. Adhering to Hume-Anderson-Kahn by removing the attack vectors against national security missions brought about by RMF, especially monitoring, intrusion detection, virus scanning, audit logging, remote administration, and remote configuration.

ii. Transitioning office automation applications into a Software-as-a-Service (SaaS) public cloud such as Microsoft and Google.

iii. Porting the network components of national security missions into an Infrastructure-as-a-Service (IaaS) public cloud such as Amazon and IBM.

iv. Enforcing zero-trust operation such that no user and no computer may adversely impact a critical mission, regardless whether the trigger is intentional or accidental.

v. Implementing Layer 8, the Mission Layer, to permit recovery from failures or attacks against Layer 7, the Application Layer.

vi. Introducing diversity and heterogeneity in the hardware and software to hedge against mono-culture failures.

Inventing the future: S&T for future missions and systems

Information assurance across the information lifecycle holds the key to mission assurance with untrusted components. As we design future missions, we must perform a trade-off between integrity and availability, as we seek execution validation for a trusted outcome.

Assuring future missions requires mathematical specification of the requirements at the far left of the acquisition lifecycle, then formal verification and testing of the implementation throughout the lifecycle. Rather than seeking resilience—recovery after every failure—we seek antifragility through information disaggregation in a public cloud[13].

To assure against supply chain threats, we must pursue system design for testability, and just-in-time mission composition. We advocate the split fabrication of integrated circuits to reduce the risk of hardware backdoors, and automatic code generation against software backdoors. Finally, we have demonstrated the utility of physics-based assurance through Physically-Unclonable Functions (PUF), ternary encryption, and practically-homomorphic encryption.

Cyber superiority at a time and place of our choosing

The later stages of conflict leading to large scale combat operations necessitate deploying a wartime reserve mode Layer 8 for contingency operations, atop a dedicated IPvMil network implementation. We envisage a three-stage development of IPvMIL to demonstrate:

(1) Cooperative deployment on Blue assets with uncontested employment,
(2) Cooperative deployment on Blue assets and Gray commons, with contested employment, and
(3) Non-cooperative deployment on Blue assets, Gray commons, and Red targets, with contested employment.

The natural progression from mathematical requirement specification and formal implementation verification is polymorphic contingency mission execution on higher-order number systems (somewhere between binary and quantum), assuring mathematical orthogonality to adversary threats.

While AI-ML-BD-C2-BM-AA serve no purpose in DCO, these technologies hold great promise for Offensive Cyber Operations (OCO) leading to cyber superiority. We advocate the development and deployment of intelligent agents capable of operating along the continuum of direct command and control (C2), automation, and autonomy.

We propose theater-scale war games informed by intelligence on adversary capability, free from the restrictions of our interpretation of adversary intent, or the illusion that defenders can detect and respond to a cyberattack in a mission-relevant timeframe. Finally, the DoD must rewrite its cyber warfare doctrine from “the way we wished it were” to “the way it actually is.” Cyber warfare must be informed by technology and enforced by technology.

Risk Analysis

The Defense Digital Service (DDS) is conducting an experiment that leverages industry best practices in computing and networking to assure selected IT applications. The post-GIG vision builds on the DDS experiment and extends it from IT applications to national security missions. We are confident that we can compose timely mission assurance from untrusted components, and assure access, integrity, and affordability, and, in the process, demonstrate that cybersecurity is neither necessary nor sufficient for mission assurance.

CONCLUSION

We propose a paradigm shift from cybersecurity through network defense, to mission assurance through information assurance, focusing primarily on assuring national security missions across the stages of conflict. We leverage age-old truths to demonstrate that cyber security is neither necessary nor sufficient for mission assurance and we recommend composing timely assurance out of untrusted components, and a shift towards commercial cloud solution.

NOTES

1. Dorothy E. Denning, "An Intrusion Detection Model", IEEE Transactions on Software Engineering, vol. SE-13, no. 2, February 1987, 222-232.
2. "System 360 – From Computers to Computer Systems", International Business Machines (IBM), https://www.ibm.com/ibm/history/ibm100/us/en/icons/system360/.
3. James P. Anderson, "Computer Security Technology Planning Study", HQ Electronic Systems Division, L.G. Hanscom Field, Bedford, MA, October 1972.
4. David Hume, "A Treatise of Human Nature", 1739.
5. Vinton G. Cerf and Robert E. Kahn, "A Protocol for Packet Network Intercommunication", IEEE Transactions on Communications, Vol. COM-22, May 1974.
6. "Managing Information Security Risks", National Institute of Standards and Technology, SP 800-39, March 2011.
7. Dr Kamal Jabbour and Maj Jenny Poisson, "Cyber Risk Assessment in Distributed Information Systems", Cyber Defense Review, Spring 2016, 79-100.
8. Dr Kamal Jabbour and Dr Erich Devendorf, "Cyber Threat Characterization", Cyber Defense Review, Fall 2017, 79-93.
9. Fred B. Schneider, "Blueprint for a Science of Cybersecurity", The Next Wave, vol 19, no 2, 2012, 47-57.
10. Dr Kamal Jabbour and Dr Sarah Muccio, "The Science of Mission Assurance", Journal of Strategic Security, vol 4, no. 2, Summer 2011, 61-74.
11. Dr Kamal Jabbour and E. Paul Ratazzi, "Does the United States Need a New Model for Cyber Deterrence?" Deterrence: Rising Powers, Rogue Regimes, and Terrorism in the Twenty-First Century, Edited by Adam B. Lowther, 2012, 33-45.
12. Dr Kamal Jabbour, "The Time has Come for the Bachelor of Science in Cyber Engineering", High Frontier: The Journal for Space and Cyberspace Professionals, vol 6, no 4, 2010, 20–23.
13. Erich Devendorf, Kayla Zeliff and Kamal Jabbour, "Characterization of Antifragility in Cyber Systems Using a Susceptibility Metric", ASME 36th Computers and Information in Engineering Conference, August 2016.