Cyber Mission Resilience

Mission Assurance in the Cyber Ecosystem

Chris Peake, Sentar Inc.
Al Underbrink, Sentar Inc.
Dr. Andrew Potter, Sentar Inc.

Abstract. Cyber Mission Resilience (CMR) is a significant step in the evolution of IT security. Not only does it reduce the complexity and cost of securing today's IT systems, it helps prioritize security-related activities. The focus on mission resilience extends the scope of past security practices while simultaneously honing in on mission-critical systems, networks, and processes. This article explores the concepts and some of the challenges related to CMR and suggests areas for future research and study.

1. Introduction

"Rapid technology advances over the past three decades and the proliferation of computers into weapon systems created a dichotomy of net-centric military superiority and a commensurate reliance on vulnerable technology" [1].

The terms "cyber" and "cyberspace" are used in everyday conversation, as well as in the media, but their meanings are vague. Most definitions describe "cyber" as groups of networks and computers. But that is not all that cyberspace embodies; it is also the "place" where people interact, share, learn, play, work, communicate, explore, buy, sell, and connect. So "cyberspace" is much more than simply a collection of networks and computers; it is also what people do with the networks and computers.

For today's Military, cyberspace is mission-critical; cyber technology is embedded in nearly every part of daily operations. But since cyber technology and information systems are sometimes vulnerable to disruption, the supported missions are also susceptible to disruptions. Current efforts to manage cyber risk focus on preventing attacks on systems and information, but this approach is reactive in nature and cannot keep pace with the threat. Nor does this approach account for the fact that systems are just as susceptible to faults, failures, and accidents that can produce the same effects as cyber attacks. This suggests that new perspectives and approaches to managing operational and cyber risk are necessary.

Most mission owners/operators realize that merely addressing system-specific vulnerabilities will not assure the mission. And they realize that effective operational risk management must consider a broader range of potentially harmful events that includes protecting systems against cyber-based faults, failures, and attacks. Therefore, achieving mission assurance in the cyber ecosystem means that mission owners/operators have a degree of confidence that their mission-critical systems will be capable of sustaining necessary operational parameters despite cyber degradation. CMR focuses on ensuring that DoD mission owners and operators trust (i.e. have confidence) that the mission-critical systems will perform as required when needed.

The Cyber Ecosystem

Achieving the CMR perspective requires that we first reconsider the cyber ecosystem as a whole. As opposed to hierarchical and stovepipe models, the cyber ecosystem is actually highly interrelated and interdependent. That is, each component both serves and depends on other aspects in the ecosystem. For example, cyber defense without intelligence regarding an adversary's offensive capabilities, and the requisite R&D/engineering capabilities, is ineffectual. Therefore, cyber defense cannot operate independent of cyber offense nor can either operate without trained personnel and governance.

In 2009 an independent study was performed by a group of IT security professionals for the U.S. Army Space and Missile Defense Command/Army Forces Strategic Command in an effort to help depict an understanding of the cyber ecosystem. The study produced a notional view of the cyber ecosystem where each functional area of cyber is highly interconnected with every other area (see Figure 1).

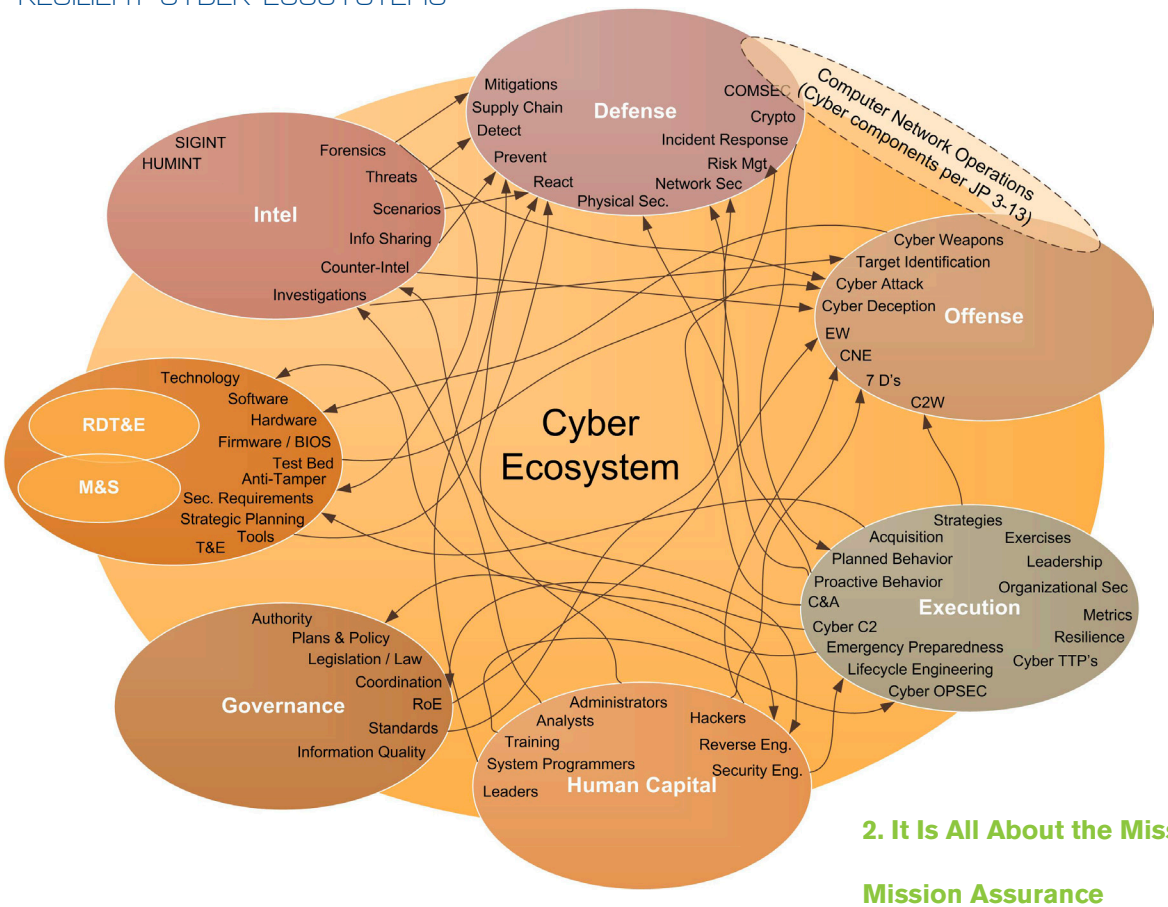


Figure 1: Notional view of the Cyber Ecosystem

Unlike the pillars of Information Operations described in Joint Publication 3-13, this view of the cyber ecosystem attempts to show the relationships among all functional areas in cyberspace. The resulting depiction of the cyber ecosystem is orders of magnitude more complex than what is expressed in current doctrine. Understanding the relationships and dependencies within the cyber ecosystem is a necessary precursor to adopting the CMR perspective.

Viewing Security as a Mission Enabler

The second step to adopting the CMR perspective is to break free from the misconception that security hampers mission functionality, and to start seeing cyber security as a mission enabler.

The mere mention of security gives most program managers and developers heartburn. For years, security has been considered a speed bump in the fast lane to project completion; security controls are thought to minimize capability, complicate architecture, and practically eliminate flexibility in system and software development. But this mindset has to change. Security should be seen as a mechanism to improve threat and fault tolerance in mission-critical system functions. Ideally, security controls should be implemented to ensure the achievement of mission objectives. Although security controls may still complicate the architecture and limit flexibility to some degree, a system developed to be more reliable, available, and dependable will be more efficacious in accomplishing the mission.

2. It Is All About the Mission

Mission Assurance

While the term "Mission Assurance" has only recently been applied to cyber, the concept itself is not new. With the increasing reliance on IT as a medium for carrying out mission objectives, there is a high probability that disruptions to information systems will have serious adverse effects on the overall mission. And despite the speed by which new software is being developed and security updates are made available, new exploits and vulnerabilities are being discovered and used even faster. In short, security professionals are losing the battle to keep our systems secure [2]. The reality is that perfect security is unattainable. Fortunately, mission-critical assets do not have to be perfectly secure; they just have to be secure enough to reliably accomplish their primary goals and objectives (i.e. their mission).

The DoD currently defines mission assurance as, "A process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan… to sustain military operations throughout the continuum of operations" [3]. This definition, while appropriate and applicable at the operational level, does not address the cyber aspects of mission assurance. If military missions depend on cyber technologies, then achieving mission assurance must also account for the mission-critical functions/tasks that are embedded in IT systems.

However, mission assurance does not guarantee mission success. It is a practice to manage operational risks that will increase the probability of achieving mission goals. As such, mission assurance can be expressed as a degree of confidence in mission success as opposed to a certainty of mission success/failure [4]. But identifying, tracking, and addressing risk, as it relates to mission goals and objectives, requires understanding the risk within the operational context (i.e. how the risk relates to achieving the mission).

The point being that mission assurance from an operational perspective cannot be achieved without assuring the cyber technologies upon which the mission depends.

Mission Resilience

The concept of mission resilience is closely related to that of mission assurance. Accenture's paper titled, "Mission Resilience: The New Imperative for High Performance in Public Service" was based on research conducted on 151 corporations and looked at how "routine disruptions" affected the organizations. While the study focused on public service organizations, the concepts presented in the paper are equally applicable to the DoD.

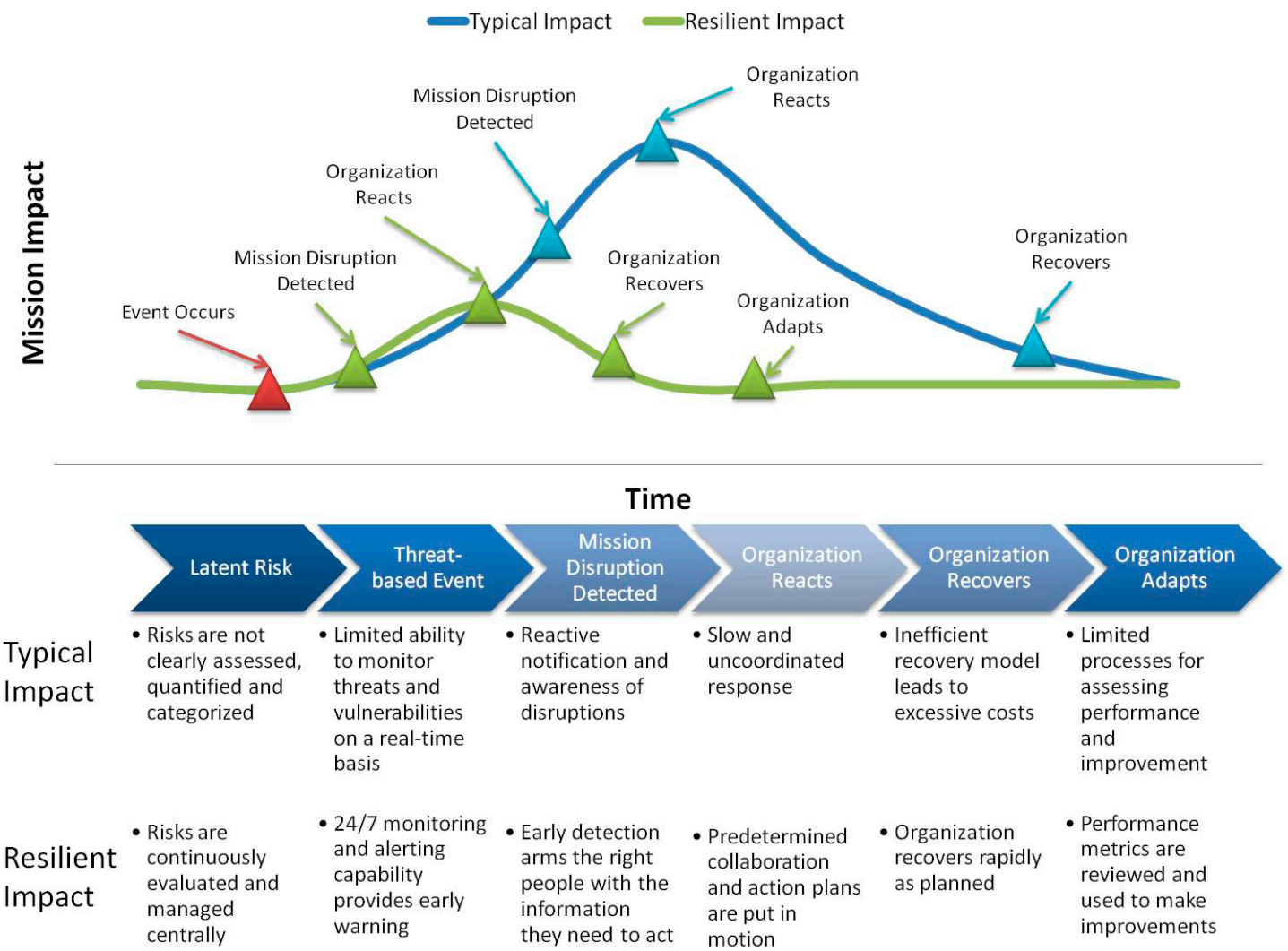
Accenture viewed mission resilience as a, "multi-tiered, life-cycle-focused methodology for understanding, anticipating, mitigating and minimizing the effects of any material disruption." Their model focuses on efficiency of mission both during normal operations and disruptive events. Unlike disaster recovery planning, mission resilience is a proactive approach that systematically prepares for potential disruptions as opposed to waiting for a disruptive event to occur.

To avoid wasting time and effort on trying to predict every possible cause of disruption, Accenture's mission resilience model focuses on protecting the mission from "symptoms" as opposed to specific events. "Building around symptoms (the effects) rather than scenarios (the causes) makes resilience development manageable because it recognizes that many events share characteristics, impacts and (most important) responses." [5] Resiliency is not necessarily about completely eliminating impacts from disruptions (or the disruptions themselves for that matter); it is concerned with minimizing impacts on the mission caused by the disruptions. If an organization or system is predisposed to handle disruptions, it can detect, react, respond, and recover more quickly to minimize the overall impact to the mission. Figure 2 depicts Accenture's resiliency capability concept; resilient organizations are able to minimize the overall impact of potentially harmful events on the mission.

Cyber Resilience

For organizations that rely upon cyber to either support or accomplish the mission, mission resilience becomes dependent

Figure 2: Accenture Resilience Capability



upon cyber resilience. Cyber resilience builds upon the properties of information assurance (i.e. availability, confidentiality, integrity, etc.) by introducing the concepts of maintainability, dependability, safety, reliability, performability[1], and survivability as aspects of system security [6]. The goal of cyber resilience is to sustain mission-critical system capabilities by applying security measures that assure the system can withstand cyber faults, failures, and attacks. Therefore, not only do mission owners need to consider a wider array of threats (i.e. faults, failures, and accidents in addition to cyber attacks), but they also need to assume these threats will affect their mission-critical systems. This assumption switches the focus from preventing cyber threats to minimizing the effects of cyber threats when they occur.

3. Achieving CMR

The concepts of mission assurance, mission resilience, and cyber resilience are, admittedly, confusingly interrelated. And while CMR may seem like just another play on words, in practice it combines the operational aspects of mission assurance and mission resilience with the technical objectives of cyber resilience. But achieving CMR requires a fundamental shift in system security processes, mindsets, controls, and tools. The following subsections discuss three tasks that need to be addressed in order to achieve CMR.

Understanding the Mission

Surprisingly, identification of an organization's mission-critical systems is not immediately self-evident. Complexity, created by the interdependence of systems, can make it difficult to determine which systems and processes are actually critical to the mission. Defining mission criticality requires identifying the impact a particular system has on overall mission success.

One tool used to help define an organization's mission, and mission critical resources, is the Business Impact Analysis[2] (BIA). While a risk assessment considers the threats and vulnerabilities associated with individual systems, the BIA is a comprehensive assessment of system functions that will reveal operational impacts, recovery time objectives, and functional dependencies of the mission critical assets. Once the BIA is complete, each mission-critical system should be assessed for its unique system protection needs.

The system protection needs are based on an examination of the potentially harmful effects (generated from the cyber threat) that can negatively impact the mission [7]. Even though most current risk assessment methodologies were developed according to information assurance-based doctrine, where "threats" referred to malicious adversaries and cyber attacks, the protection needs assessment process is equally applicable to the broader mission assurance definition of threats (e.g. system failures or faults). The key is to understand the impacts and consequences generated by the threat not necessarily the source of the threat [4].

The focus of CMR is on protecting the mission-critical systems against any event or effect that may cause a system disruption that subsequently leads to the failure to achieve mission objectives. To achieve this, it is imperative that mission owners/operators understand the mission dependencies on cyber assets and the operational parameters that are necessary to sustain the mission. In doing so, mission owners and operators are able to improve the confidence in mission success—thereby attaining a degree of mission assurance. But this is only possible if the mission and its dependencies are fully understood.

Resilience Metrics

Assurance practices are fundamentally about establishing confidence and trust, which suggests a need for qualitative and/or quantitative validation of the object being assured (i.e. assurance is not a question of belief). However, as discussed previously, assurance is not a guarantee or certainty either. But confidence and trust can be built through demonstration of reduced variation, improved dependability, consistent performance, and stable reliability. Demonstrating these qualities is a matter of repetition and statistical measurement.

As a result, cyber resilience metrics play a crucial role in achieving cyber-based mission assurance. They can be used to quantify the dependability, maintainability, safety, performability, reliability, and also the overall survivability/resilience of the mission-critical systems/functions as an assessment of mission assurance [8]. However, a comprehensive assessment of resilience requires metrics that address the full spectrum of cyber threats. Therefore, resilience metrics should also include fault measures in addition to security metrics. For example, dependability is a metric based in part on the measures of reliability and maintainability, and can address the performance of mission functions during attack or failure [9]. The aggregated metric actually provides a higher level of assurance understanding, which can be directly applied to mission objectives.

According to the Joint/Coalition Mission Thread Measures Development Standard Operating Procedure [10], the Senior Warfighters Forum (SWarF) prioritized a list of capability attributes that defines metrics in terms of mission-based functions and activities. Figure 3 depicts the SWarF attributes associated with the Net-Centric Joint Capability Area. These attributes were selected specifically because they help define how well mission activities performed. For example, enterprise IT services that are robust, scalable, interoperable, and responsive would be considered effective as a Joint capability. However, enterprise services that are unreliable due to frequent faults, failures, or cyber attacks, would be considered operationally risky. Therefore, in order for enterprise IT services to be mission assured, they must also be resilient to cyber threats.

The needed outcomes of mission assurance quantitative studies are metrics for operational fault tolerance and operational risk tolerance. Although currently not defined, the ideal measure of mission assurance would be a mission survivability or resilience rating, which would combine all other metrics (e.g. robustness, timely, agile, available, secure, etc.) into a single measure that would provide mission owners/operators with a degree of confidence in mission success.

Mission Resilience Engineering

"[Mission assurance] is an engineering process performed over the lifecycle of a program to identify and mitigate design, production, test and field support deficiencies that could affect mission success." [11]

The third task to achieving CMR is based on a lesson learned from information assurance and is summarized in the saying, "cyber security should be built-in not bolted on." Assessing mission impact, and collecting resilience metrics, cannot be accomplished unless resilience attributes are part of the system design. Mission assurance expands the scope of the system development lifecycle by making the mission objectives the driving requirements in the development process (as opposed to security controls). It combines all the necessary components of mission execution and unites them by establishing the mission as the foremost goal in system design, development, and implementation. Security is a secondary objective that is applied to improve the resilience of mission-critical systems and functions. Leveraging the mission objectives to drive system requirements actually serves to reduce overall system complexity by focusing on designing only mission essential components to be resilient [6]. Mission resilience engineering is the overarching discipline that facilitates CMR because it applies an end-to-end lifecycle approach to mission definition, requirements assessment, and metrics.

4. Conclusion

Cyberspace is a mission-critical asset in modern military operations. But the cyber ecosystem has become more complicated due to the interdependent nature of information and systems. And the threat of cyber-related faults, failures, accidents, and attacks not only makes systems unreliable but can also affect the execution of the missions that depend on those systems. Current cyber security models are unable to keep up with the ever-changing threat and as a result, our military commanders lack confidence that the mission-critical systems will be operational when needed.

A new approach is needed to reestablish confidence in the ability to deliver operationally effective and resilient cyber capabilities. CMR seeks to achieve mission assurance through mission resilience by applying engineering discipline and metrics to make cyber-based systems and capabilities resilient to faults, failures, and attacks.

NOTES

1. Performability as used in this paper and by Qian et al. is meant to convey the "ability to ensure performance" as opposed to just performance itself.
2. For additional information on the BIA refer to NIST 800-34 or ISO 27000 toolkit.

Figure 3: Net-Centric Joint Capability Attributes (JCA)

Information Transport	Enterprise Services	Net Management	Information Assurance
Accessible	Accessible	Accessible	Security
Capacity	Interoperable	Dynamic	Available
Accurate	Survivable	Flexible	Timely
Timely	Timely	Agile	Accurate
Throughput	Reliable	Integrated	Visible
Expeditionary	Accurate	Maintainable	Responsive
Latency	Relevant	Complete	Controllable
	Scalable	Reconfigurable	Complete
	Responsive		
	Robust		

REFERENCES

1. Jabbour, K. "CyberVision and Cyber Force Development." Strategic Studies Quarterly, Vol 4, No 1 2010. May 2010.
2. Lindstrom, P. "Metrics: Practical Ways to Measure Security Success." 2005. techtarget.com. 2008.
3. DoDD 3020.40. "DoD Policy and Responsibilities for Critical Infrastructure." 14 JAN 2010. FAS.org. JUN 2010. <http://www.fas.org/irp/doddir/dod/d3020_40.pdf>.
4. Alberts, C. and A Dorofee. "Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments." Sept 2005. SEI.CMU.EDU. 25 Apr 2010.
5. Accenture. "Mission Resilience: The New Imperative for High Performance in Public Service." 2008.
6. Qian, Y., D. Tipper and P., Joshi, J. Krishnamurthy. Information Assurance: Dependability and Security in Networked Systems. Morgan Kaufmann Publishing, 2007.
7. National Security Agency. "Information Assurance Technical Framework." 2002. IAD.gov. 30 Apr 2010. <https://www.iad.gov/library/iacf.cfm>.
8. Payne, S. "A Guide to Security Metrics." JUN 2006. SANS Reading Room. JUN 2010. <http://www.sans.org/reading_room/whitepapers/auditing/guide-security-metrics_55>.
9. Jaquith, A. Security Metrics: Replacing Fear, Uncertainty, and Doubt. Boston, MA: Pearson Education, Inc., 2008.
10. DISA. "Joint/Coalition Mission Thread Measures Development Standard Operating Procedure." 2010.
11. Grimm, J. "The Role of CMMI in Mission Assurance." 16 Nov 2004. DTIC.mil. 25 Apr 2010.

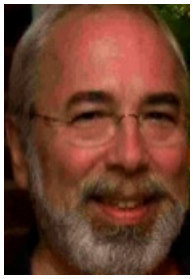
ABOUT THE AUTHORS

Chris Peake has spent the last 15 years in the IT field studying and practicing cyber security. During that time, he has supported DoD, Federal, and commercial customers by providing network, system, and security expertise. Currently, he serves as a Cyber Assurance Strategist for Huntsville-based Sentar Inc. where he supports MDA, SMDC, DARPA, SPAWAR, and other DoD/Federal customers with Information System Security Engineering, Mission Assurance, and Cyber R&D.

Sentar Inc.
315 Wynn Dr.
Huntsville, AL 35805
E-mail: chris.peake@sentar.com
Phone: 256-430-0860

Al Underbrink has been a Senior Analyst with Sentar for nine years and has served as a PI and as a technical contributor on many projects involved with research and development of secure software systems. His technical areas of expertise include computer security, information assurance, artificial intelligence, robotics, automated planning, distributed systems, model-based diagnosis and reasoning, and agent-based frameworks and systems.

Sentar Inc.
315 Wynn Dr.
Huntsville, AL 35805
Phone: 256-430-0860
E-mail: al.underbrink@sentar.com



Dr. Andrew Potter is Director of Research and Development with Sentar. Current research interests include the application of a wide range of knowledge-based and quantitative techniques to the problems of cyber security and malware analysis.

Sentar Inc.
315 Wynn Dr.
Huntsville, AL 35805
Phone: 256-430-0860
E-mail: andrew.potter@sentar.com