Cyber Situational Awareness

Major General Earl D. Matthews (USAF, Ret)
Dr. Harold J. Arata III
Mr. Brian L. Hale

INTRODUCTION

Cyberspace threats are real and growing. Worldwide cybersecurity trends and implications support these assertions: 97% of organizations analyzed in 63 countries have experienced a cyber breach; 98% of applications tested across 15 countries were vulnerable; in 2014, threat groups were present on a victim's network a median of 205 days before detection; $7.7M was the mean annualized cost of cyber crime across 252 global, benchmarked organizations in 2015; and 60% of enterprises globally spend more time and money on reactive measures versus proactive risk management.[1][2][3][4][5] "Every conflict in the world has a cyber dimension," testified ADM Michael Rogers, Commander of U.S. Cyber Command and Director of the National Security Agency, before the House Armed Services Committee in March 2015.[6] These facts, and the increasing acknowledgement regarding the importance of cyberspace on operations, place organizational leaders under immense pressure to make sound cybersecurity investment choices. Cybersecurity has truly become a political, military, economic, social, information, infrastructure, physical environment, and time concern for senior leaders.

The emergent and dynamic characteristics of cyberspace are a result of rapid advancements in computer and communication technologies, as well as the tight coupling of the cyberspace domain to physical operations. Military organizations have embedded cyberspace assets (information technology) into their mission processes as a means to increase operational efficiency, improve decision-making quality, and shorten the sensor-to-shooter cycle.[7] This cyberspace asset-to-mission dependency can place an organization's mission at risk when a cyberspace incident (e.g., the loss or manipulation of a critical information resource) occurs.

Non-military organizations typically address this type of cybersecurity risk through

Major General Earl D. Matthews (USAF, Ret) is Vice President of Hewlett Packard Enterprise's Enterprise Security Solutions Group for HPE Enterprise Services, U.S. Public Sector. In this role, General Matthews leads a team of cybersecurity experts who deliver strategic, end-to-end solutions to help HPE clients anticipate, overcome, and reduce security threats and vulnerabilities while achieving their missions. Earl Matthews is a highly decorated, award-winning retired Major General with a successful career influencing the development and application of cybersecurity and information management technology. Throughout his three-decade military career, General Matthews held many key assignments, including cyber operations, plans and policy, resource and budget management, acquisitions and staff positions.

Dr. Harold J. Arata III is the Executive for Cybersecurity Strategy at Hewlett Packard Enterprise, Enterprise Security Solutions. In this role, Dr. Arata is a key adviser to C-Suite level executives on cybersecurity strategy formulation. Prior to his arrival at Hewlett Packard Enterprise, Dr. Arata was a not-for-profit scientific research institute Cyber Center Director and was the Director–U.S. Air Force Cyberspace Technical Center of Excellence educating 650 joint cyber professionals a year. He also served as a Senior Military Professor, Air Force Institute of Technology, conducting defense-focused research at the Master's and Ph.D. levels. Preceding Dr. Arata's federal civil service, he was an active duty 2-year below-the-zone select to Full Colonel. Dr. Arata's military awards include being individually designated Best-in-Air Force as the Lt Gen Leo Marquez Communications-Electronics award winner and the Legion of Merit.

Mr. Brian L. Hale is the Associate Director for Cybersecurity Strategy at Hewlett Packard Enterprise, Enterprise Services, U.S. Public Sector, Enterprise Security Solutions. Prior to his arrival at Hewlett Packard Enterprise, Mr. Hale was the Operations Officer for a Cyber Center of Excellence at a not-for-profit scientific research institute. Preceding his career in industry, Mr. Hale was appointed as the Deputy Chief, Cyber Professional Continuing Education Division, Air Force Cyberspace Technical Center of Excellence, Air Force Institute of Technology (AFIT). Mr. Hale also served in the U.S. Air Force and retired in April 2012 after a 26-year career. Mr. Hale earned a Master of Science Degree in Information Resource Management from the AFIT, a Bachelor of Science Degree in Management/Computer Information Systems from Park University, and two associate degrees.

an introspective, enterprise-wide focused risk management program that continuously identifies, prioritizes, and documents risks so an economical set of control measures (e.g., people, processes, technology) can be selected to mitigate the risks to an acceptable level. The explicit valuation of information and cyber resources, in terms of their ability to support the organizational mission, enables the creation of a continuity of operations plan and an incident recovery plan.

While this type of planning has proven successful in static environments, military missions typically involve dynamically changing, time-sensitive, complex, coordinated operations and tasks involving multiple organizational entities. The relationship between missions, operations (military action), and tasks are shown in Figure 1.

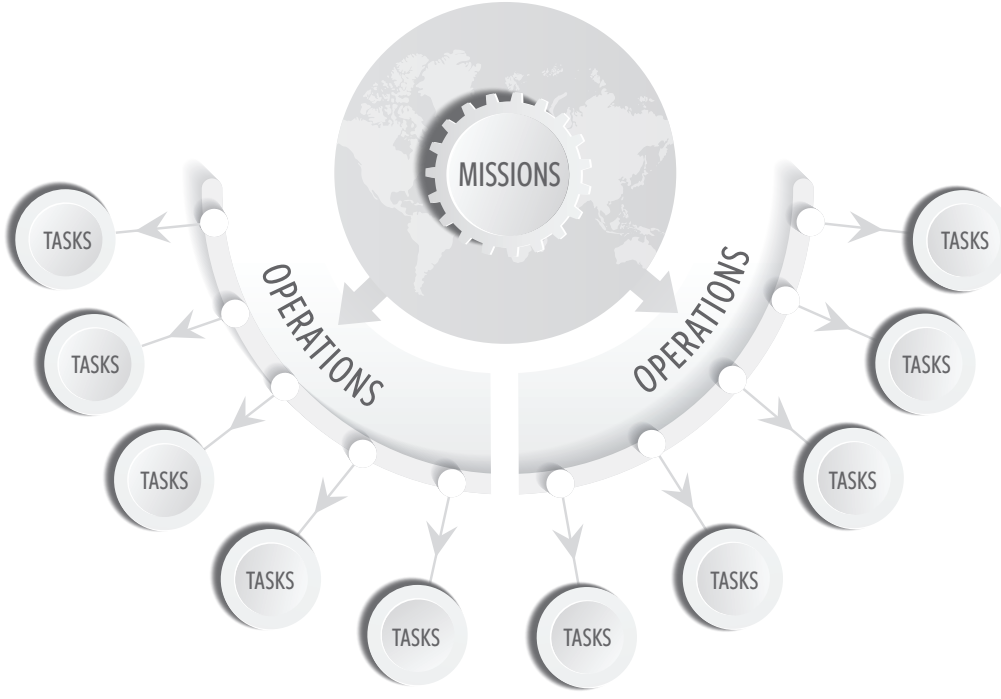

Figure 1. Relationship of missions, operations, and tasks

Mission Assurance

To assure a military organization's complex mission, several key steps must be accomplished; e.g., prioritizing mission essential functions, mapping mission dependencies on cyberspace, identifying vulnerabilities, and mitigating risk of known vulnerabilities.

It was once accepted that cybersecurity in an enterprise could only be achieved by driving out all vulnerabilities that are susceptible to exploitation. But, there is now increasing recognition this isn't necessarily the case or even possible. LTG Edward Cardon, Commanding General, U.S. Army Cyber Command, stated, "It's increasingly clear we can't protect everything."[8] Additionally, recent high-profile events in both the public and private sectors clearly demonstrate that like other threats—both natural and man-made—protecting every asset from every threat is futile and costly. As outlined in the most recent US Department of Defense (DoD) Cyber Strategy;

> Leaders must take steps to mitigate cyber risks. Governments, companies, and organizations must carefully prioritize the systems and data that they need to protect, assess risks and hazards, and make prudent investments in cybersecurity and cyber defense capabilities to achieve their security goals and objectives. Behind these defense investments, organizations of every kind must build business continuity plans and be ready to operate in a degraded cyber environment where access to networks and data is uncertain. To mitigate risks in cyberspace requires a comprehensive strategy to counter and if necessary withstand disruptive and destructive attacks.[9]

Through a risk management program, operational risks may be eliminated or reduced to an acceptable level. However, given DoD hosts 7 million networked devices and 15,000 network enclaves, and the DoD networks are probed thousands of times an hour with an ever increasing frequency and sophistication, it is likely impossible to reduce all cyberspace-related risks to zero or an acceptable level.[6][7] Rosenzweig (2009) noted even when it is feasible to eliminate risk it may be impractical because the risks are systemic and resistant to traditional cost-benefit analysis. He continued, "in a world where the identity of the threat cannot be determined with confidence, mitigation of that threat is problematic."[10]

In 2014, 97% of organizations analyzed in 63 countries have experienced a cyber breach; 98% of applications tested across 15 countries were vulnerable.

Acknowledging these challenges, as well as the difficulty of conducting risk management across an enterprise as large and complex as the DoD, a mission assurance strategy and processes, enabled by cyber situational awareness, must be employed (Figure 2).

Figure 2. Mission assurance strategy [11]

Situational Awareness and Cyber Situational Awareness

Moreover, to achieve any level of mission assurance and command and control confidence, Situational Awareness (SA) must be maximized so operational risks may be mitigated, managed, or resolved prior to a mission or during operations (reference Figure 2). SA is traditionally defined following the pioneering and influential work of Mica Ensley in 1988; SA is a long-studied field concerned with the perception of the surroundings and derivative implications critical to decision makers in complex, dynamic areas such as military command and security.[12]

Given the progressive and usefulness of SA research, SA is being applied to cyberspace. To this end, and in concurrence with Franke and Brynielsson (2014), cyber SA is posited to be a subset of SA.[13] Through a holistic SA approach, the combination of information from different disciplines, e.g., human intelligence, geospatial intelligence, and open source intelligence, can be combined with cyberspace sensor information (e.g., intrusion detection system alerts) to enhance overall cyber SA. The concepts and strategy for achieving cyber SA requires disciplined processes, enabling technologies, and collaborative organizations.

Wanted: New Thinking in Cybersecurity and Cyber SA

While the sophistication of cyber threats facing governments and industry grows every day, traditional thinking about how cybersecurity leaders should fight that challenge is evolving. Longstanding assumptions and tired orthodoxies aside, cybersecurity and cyber SA means building new frameworks from the ground up to include reinventing an organizations ability to understand mission dependences and cyber threat landscapes,

reforming of training and cyberspace operator qualifications, as well as the refashioning of supporting network tools that enable an organization's personnel to operate at the speed of light–netspeed. Commanders recognize status-quo thinking and incremental change rarely keeps pace with an aggressive adversary.

Cyber SA can be a complex and bewildering topic for policy makers not used to working within the daily cyberspace ecosystem. However, by applying "well-recognized risk management principles commonly used in other security domains, such as transportation and port security, and comparing the approach to dealing with other predatory and adaptive threats, including terrorists and foreign intelligence services, a clearer picture emerges."[14] What matters in transforming an organization's cyber SA is intelligence, integration, speed, analytics, expertise, and resiliency (Table 1). Simply stated, no single countermeasure is effective against every threat. Resourcing cybersecurity and cyber SA becomes a matter of sound risk management decisions, based on threats and vulnerabilities to data, applications, systems, and networks that have the highest likelihood of impacting mission assurance.

Table 1. What matters in transforming your cyber SA mission space

Intelligence Matters	Rely on up-to-the-minute threat intelligence to proactively understand threats to your cyber SA enterprise. Achieved through actionable threat research and commercial threat intelligence sensor grid and network analysis.
Integration Matters	Automated synthesis of SA monitoring information from across your enterprise infrastructure, operational and intelligence processes, and applications. Achieved through integrating data flows into a continuous monitoring platform.
Speed Matters	Breaches are inevitable; cyber SA assessments, automation, and analytics reduce reaction time and mitigate damage to your enterprise. Achieved through innovative analytics.
Analytics Matters	Ingest data to analyze, correlate, and visualize events to produce actionable, contextual, scalable, and insightful cyber SA. Achieved through analytics platforms that leverage devices and their data as assets, moving organizations from being reactive to proactive across their operations.
Expertise Matters	Leverage industry cyber SA expertise to help better understand vulnerabilities, manage threats, and achieve mission assurance. Achieved through support, managed services, training, and education.
Resiliency Matters	Be prepared for the unexpected by protecting your data confidentiality, integrity, and availability. Cyber SA achieved through end-to-end data protections, virtualization, and continuity plans.

An escalating number of industry insiders believe more creative thinking, more research, more knowledge management and more SA—not just more technology—is needed. Dr. Thomas Homer-Dixon outlined just such an ingenuity gap, "in general, as the human-made and natural systems we depend upon become more complex, and as our demands on them increase, the institutions and technologies we use to manage them must become more complex too, which further boosts our need for ingenuity. The crush of information in our everyday lives is shortening our attention span, limiting the time we have to reflect."[15] It is these increasing demands, combined with today's greater network complexity, and rising social unpredictability, that make it more critical than ever that smart technical and social solutions be ready at a moment's notice. The MIT scientist Edward Lorenz's Chaos theory is also used to describe how small changes can lead to widely varying results and path dependence.[16] As such, it is essential to leverage a new cyber SA model that incorporates the aforementioned: intelligence, integration, speed, analytics, expertise, and resiliency.

No single countermeasure is effective against every threat. Cybersecurity and cyber SA becomes a matter of sound risk management decisions.

For example, the new cyber SA model may include leveraging industry threat intelligence feeds and analysis integrating millions of sensors, with the capability to analyze billions of files, web objects and flows per day, while continuously sharing those results within the organization and externally with its' partners. The benefits of commercial intelligence feeds are overwhelming, both qualitatively and quantitatively, compared to today's military sensor collections. Additionally, there is a reluctance by many organizational partners to share intelligence data due to their sources and methods. Michael Daniel, the White House cybersecurity coordinator, described information sharing as "critical to effective cybersecurity," and the Cybersecurity Act of 2015 was passed in December 2015 to provision this information sharing.[17][18]

Cybersecurity has traditionally worked from a defensive position, supported by an industry whose default mode is to patch, prevent, block and build *improved* versions of the same technology. This innovation deficit on the part of the industry has impacted end users, military commanders, chief information officers, and chief information and security officers who are trying to build mission assurance security strategies against unprecedented threat levels. A great number of organizations still have a security strategy that was formulated when the concepts of intelligence, integration, speed, analytics, expertise, and resiliency were not fully understood. With President Obama's recent call for a 30-day sprint in July of 2015 to improve government-wide cybersecurity perfor-

mance after the Office of Personnel Management compromise, cybersecurity experts believe it is "unlikely agencies can solve in a month a problem that's been festering below the radar for years." [19] Alan Paller, Director of SANS Institute, stated, "If you come back in a few months, you will see that the change has slowed radically because OMB [Office of Management and Budget] will go on to other metrics." [20] Organizations need to step-up with accelerated, sustained, and measured cybersecurity efforts.

For example, most public sector requirements and requirements processing, which is a 2-to-10 year cycle, has to accelerate in support of a rapid cyber acquisition model that can keep pace with the quantum leap in technology advances from year-to-year. Furthermore, a typical 5-year DoD Future Years Defense Program (FYDP) planning and budgeting cycle is not rapid, considering advances in cyberspace technologies consistently double every 2-3 years when put in the context of observations of Moore's and Bezos' laws (Figure 3).

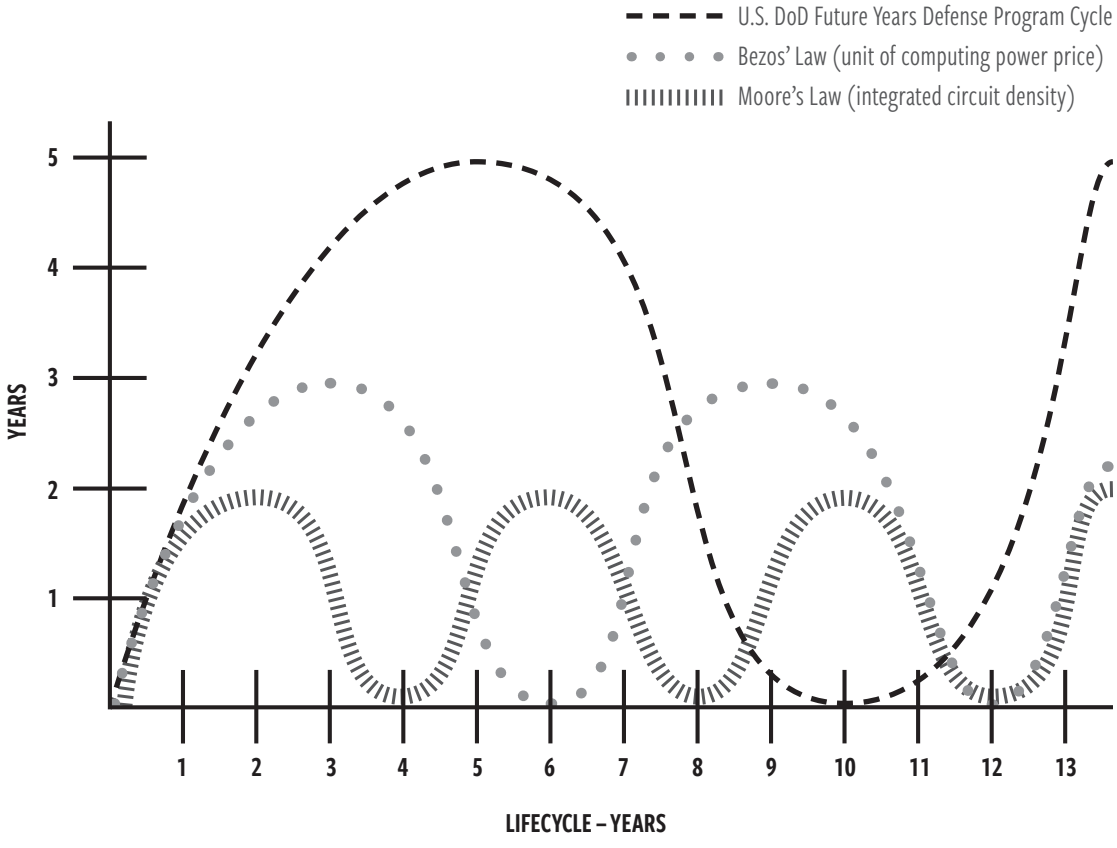

Figure 3. Comparison between rapid technology developments and the requirements capability document FYDP process

Looking ahead, technology continues to enhance mission capabilities in numerous ways, and with that comes the critical challenge of maintaining cybersecurity throughout on-going missions, operations, and tasks. However, with increased cooperation and innovative thinking, a thorough understanding of the imminent cyberspace threats to mission assurance may be achieved.

Through an effective cyber SA lifecycle, like the proposed framework in Figure 4, any organization can further enhance mission assurance by improving the timeliness, relevance of notification, and incident response following a cyberspace incident. Moreover, a cyber SA warning capability may prevent a cyberspace incident from occurring.

A cyber SA framework defines appropriate security metrics, security enforcement policies, controls and technologies, security management, operations workflow, and multi-level risk management reporting dashboards that can fuse and address these and many more complex issues facing current organizations both in the private and public sectors.

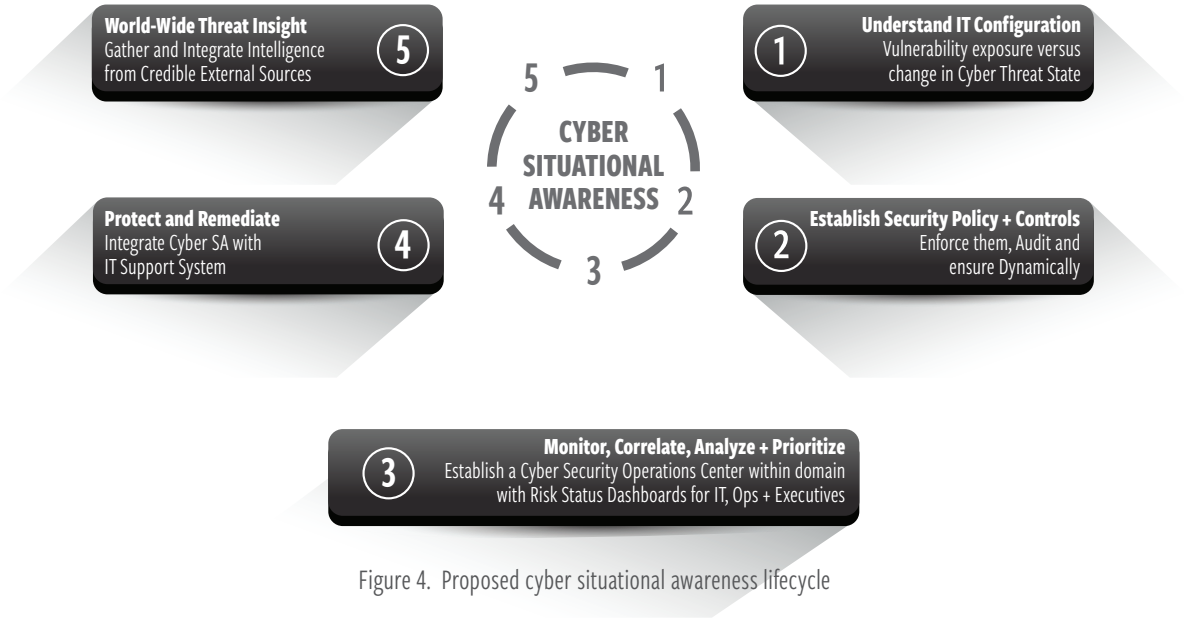

Figure 4. Proposed cyber situational awareness lifecycle

CONCLUSION

Protecting enterprise networks and providing mission assurance without a significant cyber SA and warning capability will continue to be a challenging mission. Without cyber SA, a fragmented, imperfect view into enterprise networks and how cyber assets map to tasks, objectives, and missions occurs. This incomplete view thwarts threat detection, trend analysis, and preemptive actions creating slow or non-existent reactions to threats and changing conditions thereby constricting a senior leader's decision-making space.

Cyber SA for most enterprises are presently disjointed, rudimentary, ad hoc, too focused on technical analysis, lacking important cyber threat intelligence data feeds from supporting providers, and missing actionable, contextual analytics. Moreover, personnel are currently delivering very limited strategic cyber SA capabilities for senior leadership. This flawed view can be operationally blinding to any organization.

Initial progress has been made today by many organizations to increase their cyber SA capability, for example, with the implementation of security operations centers. However, most organizations may further strengthen their cyber SA and warning capability by incorporating commercial cyber threat intelligence capabilities, bolstering their cyber SA structures, implementing a comprehensive cyber workforce education and certification program, fusing cyber SA data into actionable information (tactical, operational, and strategic dashboards), and recognizing cyberspace as a domain. By weaving an enabled mission assurance strategy with an empowered cyber SA construct is a high return on investment for any organization operating in today's high threat environment.

The time has arrived for a new model, more ingenuity, and recognizing the importance of cyber SA in defense of an organization's enterprise. What matters in transforming an organization's cyber SA is intelligence, integration, speed, analytics, expertise, and resiliency. Enacting just such a cyber SA framework can and will enable an organization to more effectively protect itself both today and into its' future.

Timeless Senior Leader Insights

Dave Packard, one of Hewlett-Packard founders, stated, "It is necessary that people work together in unison toward common objectives and avoid working at cross purposes at all levels if the ultimate in efficiency and achievement is to be obtained."[21] This is part of Hewlett Packard Enterprise's core company objectives and shared values: transform to a hybrid infrastructure; protect your digital enterprise; enable workplace productivity; empower the data-driven organization. Hewlett Packard Enterprise believes this is especially the case for enhancing cybersecurity and cyber SA. Success will depend on a common effort by all stakeholders. Hewlett Packard Enterprise is committed to working with legislators, agencies, clients and citizens to achieve this most important objective.

The views expressed are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

NOTES

1. FireEye and Mandiant, A FireEye Company. Cybersecurity's *Maginot Line: A Real-World Assessment of the Defense-in-Depth Model.* Retrieved from http://www2.fireeye.com/rs/fireye/images/fireeye-real-world-assessment.pdf. (accessed 2015).
2. Trustwave. *Trustwave Global Security Report.* Retrieved from https://www2.trustwave.com/rs/815-RFM-693/images/2015_TrustwaveGlobalSecurityReport.pdf. (accessed 2015).
3. Mandiant, A FireEye Company. *M-Trends 2015: A view from the front lines.* Retrieved from https://www2.fireeye.com/rs/fireye/images/rpt-m-trends-2015.pdf. (accessed 2015).
4. Ponemon Institute, & Hewlett Packard Enterprise. 2015 *Cost of Cyber Crime Study: Global.* Retrieved from http://www8.hp.com/us/en/software-solutions/ponemon-cyber-security-report/ (accessed October, 2015).
5. Hewlett Packard Enterprise. *Protecting your business with a more mature IT security strategy.* Retrieved from http://www8.hp.com/h20195/v2/GetPDF.aspx/4AA5-5744ENN.pdf. (accessed November, 2015).
6. Pellerin, C. CYBERCOM Chief: Cyber Threats Blur Roles, Relationships. *DoD News.* Retrieved from http://www.defense.gov/News-Article-View/Article/604225 (accessed March 6, 2015).
7. National Institute of Standards and Technology. Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34, Revision 1. (Gaithersburg, MD: Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, U.S. Department of Commerce, 2010).
8. Cardon, Edward, Lt. Gen. Cyber can't protect everything. *Signal, Armed Forces Communications Electronics Association.* Retrieved from http://www.afcea.org/content/?q=cyber-cant-protect-everything (accessed 2014).
9. Carter, A. *The DoD Cyber Strategy.* Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. (accessed April 17, 2015).
10. Rosenzweig, P. *National Security Threats in Cyberspace—Post Workshop Report.* Retrieved from http://www.abanet.org/natsecurity/threats_%20in_cyberspace.pdf (accessed 2009).
11. Alberts, C.J. & Dorofee, A.J. *Mission Assurance Analysis Protocol (MAAP): Assessing Risk in Complex Environments.* Carnegie Mellon University Networked Systems Survivability Program Report CMU/SEI-2005-TN-032, 2005.
12. Endsley, M. R. Design and evaluation for situation awareness enhancement. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (SAGE Publications Vol. 32, No. 2, 1988) 97-101.
13. Franke, U., & Brynielsson, J. Cyber situational awareness–a systematic review of the literature. (*Computers & Security,* 2014) 46, 18-31.
14. Hewlett Packard Enterprise. *National Cybersecurity State Policy Leadership Managing risk in the Cyber World, (Hewlett Packard Business White Paper, 2012)* 3.
15. Dixon, H. The ingenuity gap, How can we solve the problems of the future? (New York, NY: Knopf Publishing, 2000).
16. Lorenz, E. *Predictability: Does the Flap of a Butterfly's Wings in Brazil Set Off a Tornado in Texas?* 1972 Retrieved from http://eaps4.mit.edu/research/Lorenz/Butterfly_1972.pdf.
17. Fischer, E. *Federal Laws Relating to Cybersecurity: Overview of Major Issues, Current Laws, and Proposed Legislation;* Congressional Research Service CRS Report R42114. Retrieved from https://www.fas.org/sgp/crs/natsec/R42114.pdf. (accessed 2015).
18. Consolidated Appropriations Act of 2016, H.R.2029, 114th Congress. Retrieved from https://www.congress.gov/bill/114th-congress/house-bill/2029 (accessed 2015).
19. Golden, H. *Security Experts Point to OPM's Biggest Cybersecurity Failure.* Retrieved from http://www.nextgov.com/cybersecurity/2015/07/security-experts-point-opms-biggest-cybersecurity-failure/118274/ (accessed July 21, 2015).
20. O'Connell, M. *Where do agencies go now post-cyber sprint?* Retrieved from http://federalnewsradio.com/cybersecurity/2015/08/agencies-go-now-post-cyber-sprint/ (accessed August 4, 2015).
21. Packard, D. *HP Corporate Objectives and Shared Values. 1957* http://www.hp.com/hpinfo/abouthp/values-objectives.