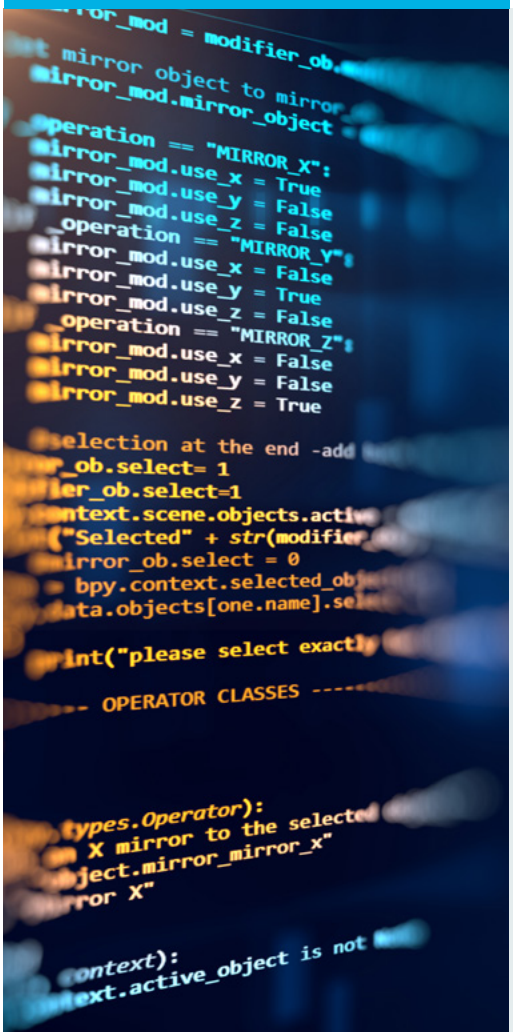
White Paper

Vulnerability Analysis and Operations: A New Approach to Supporting Converged Cyber Operations

By Samuel Visner, ICF



Overview

Two important developments call for a new approach to the National Security Agency (NSA) Vulnerability Analysis and Operations (VAO) effort:

First, NSA is converging its defense and offensive cyber operations and capabilities to reflect the changing nature of cyberspace as an operational domain. In this domain, defense and exploit operations share the same environment, and common capabilities must be developed and employed.

Second, the cyberspace environment in which NSA must operate—where it must defend its own capabilities and conduct intelligence operations—is an operational domain it shares globally with friends, stakeholders, and adversaries. Today's cyber-enabled world does not have a "forward edge of battle," as it does not permit us to separate our civilian infrastructure and economy from the operational battlespace where military operations take place. In seeking technological, military, economic, and other advantages, adversaries operate against our military, civil government, research and development enterprises, critical infrastructure, and private sector economy. The domain that serves these sectors supports the widest possible range of vital activities—from civilian research and development to military mobilization—often with little regard to national boundaries. NSA's decision to build converged operational capabilities demands a modern approach to VAO. This paper describes such an approach.

Discussion

Breaches occur. Infrastructures are increasing in size and complexity, leading to new attack surfaces. Changes in policy and increased public concern, coupled with a critical need for experienced cybersecurity experts, means that leaders must rethink how to most effectively protect their data. Vulnerability assessments—both pre- and post-breach—are increasing in importance.

An offensive cyber-operations perspective requires detecting vulnerabilities to provide insights into new tools for intelligence—tools that can take advantage of the opportunities that larger and more complex infrastructures create.

The Future of VAO

Shaping Forces

Foremost among shaping forces changing the environment is the confluence of all network operations—and the inherent capabilities to defend, exploit, and attack—often in a highly orchestrated and simultaneous manner. This is a goal that NSA's reorganization for the 21st century (NSA21) is working to reach. Like a battlefield soldier who can attack, defend, or reconnoiter whenever necessary, NSA21's confluence of capabilities must be ready for any aspect of the cybermission for which the agency is responsible. Adding to this challenge, the infrastructures that are being attacked/defended/exploited are more complex, more likely in the cloud, more likely connected to the Internet of Things, and are constantly changing. This complexity is amplified by the adoption of the IPv6 protocol and the increase in zero-day exploits.

The sheer volume and acceleration of cyberthreats is staggering. According to a recent report by Symantec[1], the number of attacks that exploited previously unknown software vulnerabilities more than doubled in 2015 as hackers found effective ways to infect end users with malware. Data are compromised on an unprecedented scale, with nine reported cases in 2015 of major data breaches that compromised 429 million personal records. Crypto-ransomware attacks climbed by 35 percent, and more than 430 million variants of malware were uncovered. The size and complexity of today's networks, coupled with the rise of advanced malware, challenge existing vulnerability assessment models.

What This Means for VAO, and What Can Be Done

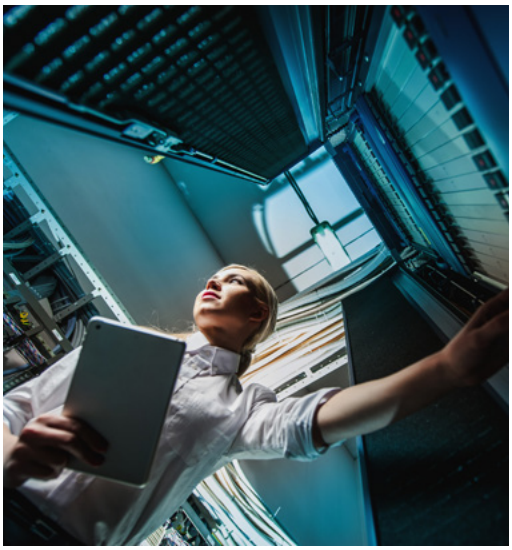
Challenges to the VAO effort continue to mount as more resources are needed to address customer and shareholder needs. Whether performing network or application vulnerability assessments, reverse engineering, or penetration testing, every vulnerability should also be seen as an opportunity. Each might provide insight into who might be vulnerable to the same discovered weaknesses.

To keep pace with the speed of exploitation, a close link between VAO and the Research Directorate can facilitate rapid insertion of new methodologies

[1] Symantec Internet Security Threat Report, Volume 21, April 2016.

 ©Copyright 2016 ICF

and diverse technologies to mitigate intrusions and reduce vulnerability consequences. Beyond capable people with superior training, advanced network emulation and analysis tools with more capability would be able to assess a network quickly within its established edges and determine possible attack vectors through entry points; running services; and identity, credentialing, and access management utilization. The use of automation to achieve resiliency—as well as risk and breach detection/mitigation capability—is of paramount importance, particularly for complex systems operating at the intersection of traditional information technology (IT) and operational technology (OT). Use of tools such as FIRELAMP, on which ICF has worked at the Air Force Research Laboratory, allows for greater fidelity in studying the behavior of such systems and in assessing their potential vulnerabilities.



The move toward more exacting cybersecurity education (and educational standards and certification) can also convey benefit to the VAO effort. This effort should consider an approach that provides access to professionals with this education and associated certifications. Such professionals could aid in swifter identification and resolution of vulnerabilities.

NSA currently conducts large audience conferences, such as the Information Assurance Symposium and the ReBI Symposium. While the information exchanged at these conferences is useful, smaller and more focused technical collaboration events—classified and unclassified—could focus attention on key area(s) of interest.

A systematic process for obtaining input from the different directorates (operations, capabilities, and research), industry, and interested U.S. government entities—including the Army, Air Force, and Navy research laboratories, and possibly Department of Energy national laboratories—could enhance VAO's capability. A board representing these entities could help provide strategic advice on relevant technology, including critical infrastructure, operational military technology, emerging standards, and research and development efforts useful to the VAO mission.

Acquisition Strategy

Services acquired under the VAO effort are likely to be broader than those encompassed by the current contract and range from routine operations to advanced technical approaches. Such an approach would reflect the broad outlines of NSA21 and serve the increasingly converged approach to defense and offensive cyber operations and capabilities resulting from NSA's new organizational alignment. Through ID/IQ contracts, the government will be able to periodically compare multiple technical approaches to task areas that will only become increasingly complex. This strategy would provide government flexibility, offering access to a variety of companies with a range of capabilities appropriate to the widening range of VAO needs. The SCOOBYSNACKS effort is an example of this approach.

 ©Copyright 2016 ICF

In addition, some services provided under the new VAO contract may be excellent candidates for outcome-based procurement, as measureable performance standards can be tied to required outcomes.

For years, our team of top cybersecurity specialists has helped intelligence and military clients successfully defend the most aggressively attacked infrastructure on the planet. But the benefits of our work extend far beyond this complex challenge.

We adapt our proven strategies for organizations of all sizes across various industries. Collaborating with ICF's subject matter experts in specific markets, our cybersecurity teams design programs, advise on policies, and work on site to implement custom, scalable solutions.

Whether securing an energy grid, transportation system, defense network, or private healthcare information, ICF helps clients mount a sophisticated defense.

What ICF Brings to VAO

1. **Large Computer Network Defense Service Provider (CNDSP) capabilities and experience.** We are one of the largest CNDSPs serving the Department of Defense (DoD), protecting a number of key networks, including the Defense Research Engineering Network.
2. **Advanced network modeling capability.** Our efforts, including FIRELAMP, give us the means to emulate and assess the vulnerabilities of very complex IT/OT networks.
3. **Substantial network vulnerability assessment through CNDSP.** Our CNDSP teams' forensics capabilities—as well as our ability to characterize networks prior to instituting new computer network defense measures—gives us the experience to analyze the operational networks of interest to NSA.
4. **Partnerships with companies that have advanced capabilities for network and malware analysis.** ICF has formed partnerships with companies and academic and research institutions, pioneering new approaches to modeling network performance and assessing network vulnerabilities. Our October 2016 CyberSci cyber research and development symposium will provide a showcase for the expertise we are building with our network of affiliated companies and institutions.
5. **Extensive cyber research and development.** More than 140 of our people are currently working with the Army Research Laboratory (ARL). In addition, our professionals are working with the Air Force Research Laboratory for advanced network behavioral modeling under the FIRELAMP efforts.
6. **Links to critical infrastructure, particularly energy.** ICF is currently active with the Department of Energy in the development of a cybersecurity capability maturity model for electrical energy cybersecurity. Our professionals work throughout the electrical power industry to put in place programs that are consistent with North American Electric Reliability Corporation's Critical Infrastructure Protection standards to overcome cyber vulnerabilities.

In addition, ICF participates in the frontline defense of major DoD organizations, leveraging our strong capabilities in network monitoring and defense; innovative research into the science of offensive and defensive network operations; threat and vulnerability analysis and forensics; identity management; and compliance and remediation.

For more than 16 years, ICF has provided cyberdefense expertise in supporting cybersecurity programs for organizations including ARL, the Department of Veterans Affairs, the Federal Emergency Management Agency, and the Federal Trade Commission. Our cybersecurity subject matter experts employ a hands-on, proactive,

 ©Copyright 2016 ICF

About ICF

ICF (NASDAQ:ICFI) is a global consulting and technology services provider with nearly 6,000 professionals focused on making big things possible for our clients. We are business analysts, public policy experts, technologists, researchers, digital strategists, social scientists, and creatives. Since 1969, government and commercial clients have worked with ICF to overcome their toughest challenges on issues that matter profoundly to their success. Come engage with us at **icf.com**.

For more information, contact:

Samuel Sanders Visner
samuel.visner@icf.com

risk-reducing approach to maintaining the confidentiality, integrity, and availability of IT assets through the use of industry-standard tools as well as customized tools created by ICF's software developers. In addition, our commercial cybersecurity practice is helping assess the vulnerability of private-sector networks, including those of the nation's electrical power grid.

Our staff develops and integrates tools for the Army to protect the DoD Information Network. ICF augmented ARL's cybersecurity capabilities and played a major role in helping ARL to achieve certification as a computer network defense service provider within DoD. One of our major accomplishments is the research and development of the robust and flexible Intrusion Detection System utilized by the ARL CNDSP group, enabling rapid prototyping and integration of new operational components as demanded by the mission.

ICF actively supports multiple DoD organizations in the transition from the DoD Information Assurance and Accreditation Process (DIACAP) to the Risk Management Framework (RMF), as mandated by DoD 8510.01 dated March 12, 2014. With the DoD transition from the DIACAP Certification and Accreditation Process to the RMF, ICF cybersecurity subject matter experts support these efforts by conducting Assessment and Authorization (A&A) evaluations within both CONUS and OCONUS. The A&A process ensures that appropriate controls are implemented to safeguard the confidentiality, integrity, and availability of sensitive and classified information systems on an ongoing basis.

Summary

VAO will exist in a new operational and organizational context, one that reflects the converged nature of cyber operations as well as the changing global IT infrastructure environment NSA faces. VAO will continue to need broader capabilities. We hope the ideas we have presented here help in developing an acquisition strategy to gain those capabilities, helping VAO meet this ever-widening challenge.

We look forward to discussing and elaborating on these ideas with NSA as the government prepares for the next generation of VAO services.

Any views or opinions expressed in this white paper are solely those of the author(s) and do not necessarily represent those of ICF. This white paper is provided for informational purposes only and the contents are subject to change without notice. No contractual obligations are formed directly or indirectly by this document. ICF MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

No part of this document may be reproduced or transmitted in any form, or by any means (electronic, mechanical, or otherwise), for any purpose without prior written permission.

ICF and ICF INTERNATIONAL are registered trademarks of ICF and/or its affiliates. Other names may be trademarks of their respective owners.