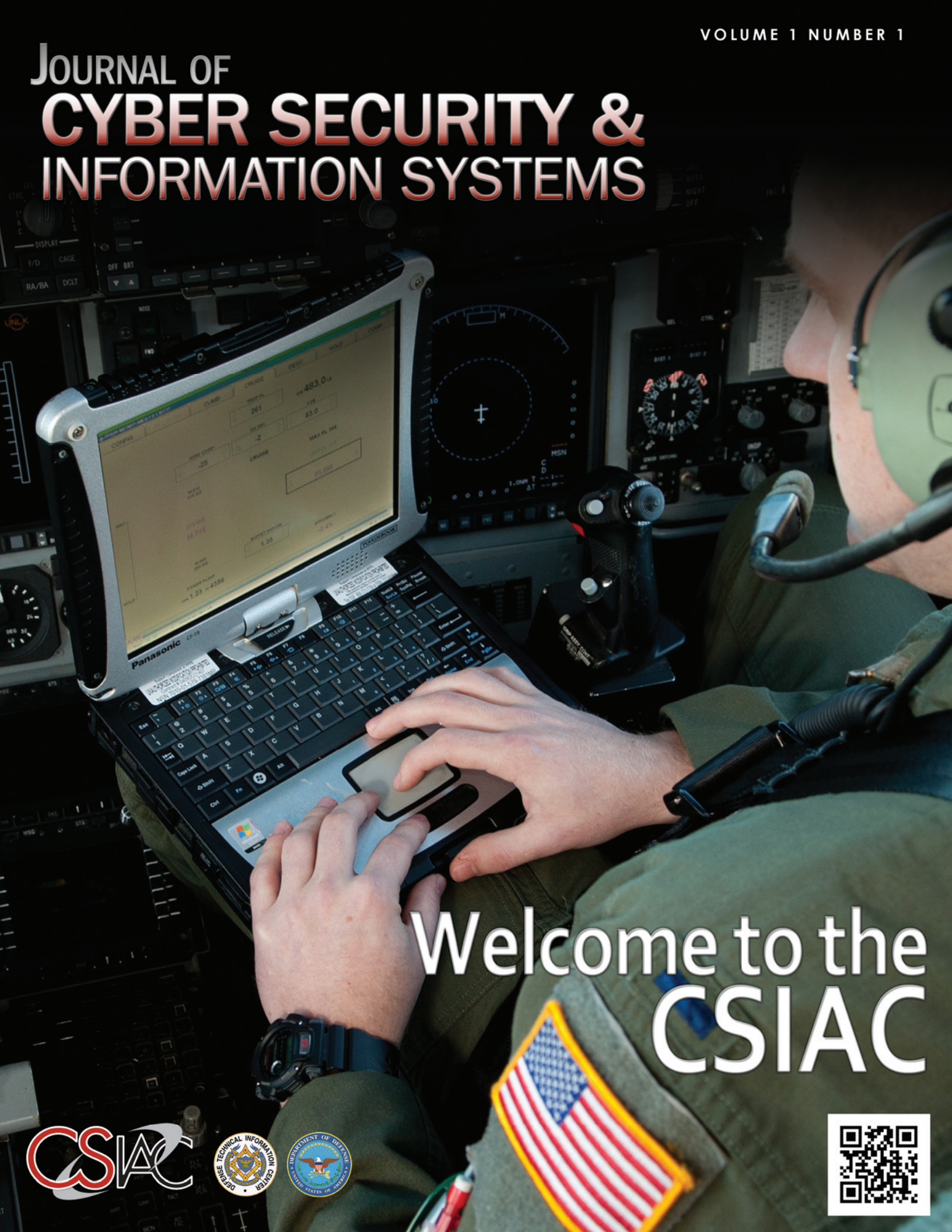
VOLUME 1 NUMBER 1

JOURNAL OF CYBER SECURITY & INFORMATION SYSTEMS



Welcome to the CSIAC

Welcome to the New and Enhanced Cyber Security and Information Systems Information Analysis Center - CSIAC

By Christopher Zember, Deputy Director, DoD Information Analysis Centers, and
Thomas McGibbon, CSIAC Director, Quanterion Solutions Inc.

Change is in the Air: A New IAC Has Been Formed for You - CSIAC

You are receiving this new *Journal of Cyber Security and Information Systems* from the Cyber Security and Information Systems Information Analysis Center (CSIAC) because you have previously been a user of information from or a subscriber to newsletters or journals from the Data & Analysis Center for Software (**DACS**), the Information Assurance Technology Analysis Center (**IATAC**), or the Modeling & Simulation Information Analysis Center (**MSIAC**). Of the previous 10 Information Analysis Centers (IACs), DACS, IATAC, and MSIAC have been consolidated to form the new CSIAC.

Given the evolving Defense environment, as well as recent congressional guidance, the Defense Technical Information Center (DTIC) recognized an opportunity to reshape the IACs to better respond to DoD mission needs. As a result, DTIC is realigning and consolidating the IAC program structure to achieve several objectives:

- Expand the IAC program scope and increase synergy across related technology areas
- Increase opportunities for small business
- Expand the industrial base accessible through the IACs

To achieve these objectives, DTIC is forming new, consolidated IAC Basic Centers of Operation (BCOs). The BCOs are managed by both industry and academia. The DoD establishes IAC BCOs in areas of strategic importance, such as cyber security and information systems. An IAC BCO serves as the center for its technical community, and as such must maintain connection with all of the key stakeholders within that community, in order to understand on-going activities, current information, future strategies and information needs.

This mission remains unchanged in the new IAC structure. However, what the new approach brings is expanded scope, increased focus on technical information needs, and enhanced agility, as the Defense environment continues to evolve.

BCOs will still analyze and synthesize scientific and technical information (STI). However, they also are to take on an expanded role in program analysis and integration by assessing and shaping nearly $6 billion in Technical Area Tasks (TATs). TATs are a companion offering of the IAC Program, by which DTIC leverages industry and academia's best and brightest to conduct research and analysis, developing innovative solutions to the most challenging requirements. IAC BCOs will ensure consistency with and reduce duplication of prior or other ongoing work and by helping to ensure TATs are more responsive both to customer needs and broader DoD imperatives. BCOs also are to ensure that TAT results are properly documented and made available for broad dissemination. This approach both achieves cost savings and reduces risks, ensuring that in this time of shrinking budgets and evolving requirements, the Defense community leverages all available knowledge to identify and implement innovative solutions.

Enter CSIAC

The CSIAC BCO represents the first awarded BCO under the new DTIC structure. As its name suggests, CSIAC's main technical focus is in Cyber Security and Information Systems. CSIAC merges the software engineering technology area of the DACS, the modeling & simulation technology area of the MSIAC, and the information assurance technology area of the IATAC. It will also address two new technology focus areas: knowledge management and information sharing. Additionally, CSIAC will expand into other areas of importance and closely monitor new technologies as they emerge.

The CSIAC is focused on leveraging knowledge bases, best practices and expertise from industry, government and academia in each of the technology domains it covers. CSIAC will draw on the knowledge databases of the legacy IACs, including many thousands of holdings of scientific and technical information, along with a well-established community of experts across the globe.

With a new IAC come new opportunities and initiatives. The remainder of this article will focus on some of the major initiatives being supported by DTIC under the CSIAC program.

Better Buying Power (BBP) and IACs

As discussed in a recent report on IACs from the Center for Strategic and International Studies (CSIS)[1], affordability is a top challenge facing the Department of Defense (DoD) today as amplified by the following comments from Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L)) Frank Kendall in continuing to emphasize reducing defense system costs:

> *"We will continue to refine and build upon [the Better Buying Power Initiative]. We will continue the never-ending quest to control and reduce our costs while acquiring products and services that provide the highest possible value to our warfighters."*[2]

CSIS conducted a detailed assessment of changes underway within the IAC Program. Their review concluded that under the new consolidated, restructured, and enhanced construct, BCOs are positioned to create and sustain a focus on the BBP Initiative to improve affordability, productivity, and standardization within defense acquisition programs. Additional information, as well as a link to the CSIS report, can be found at: **http://iac.dtic.mil/better_buying_power.html** CSIAC will continue to identify and optimize opportunities for the IACs to more directly support the DoD acquisition community and the acquisition affordability imperative.

Data as a Critical Service to Better Buying Power

One of the BBP initiatives that was initiated under the DACS BCO program to be continued and expanded under the CSIAC BCO is the **Software & Systems Cost and Performance Analysis Toolkit (S²CPAT)**.

The goal of S²CPAT is to capture and analyze software engineering data from completed software projects that can be used to improve a) the quality of software –intensive systems and b) the ability to predict the development of software – intensive systems with respect to effort and schedule. S²CPAT currently allows users to search for similar software projects and use the data to support:

1. Rough order of magnitude estimates for software development effort and schedule
2. Project planning and management: life cycle model information, key risks, lessons learned, templates, estimation heuristics
3. Software engineering research

The S²CPAT repository contains Software Resources Data Report (SRDR) data provided by the US Air Force. This data has been sanitized for public release by DoD and validated by a DoD-funded academic research team. Access to the S²CPAT can be found through the CSIAC website.

The effort was recognized in the CSIS study[1] as "… an example of the significant benefits of the new IAC construct, including increased support to the BBP Initiative."

1 "A Case Study for Better Buying Power: Information Analysis Centers of the Defense Technical Information Center;" The CSIS Defense-Industrial Initiatives Group; April 2012, ISBN 978-0-89206-735-0, http://csis.org/publication/case-study-better-buying-power

2 "Initial Guidance from the Acting Under Secretary of Defense for Acquisition, Technology and Logistics (USD(AT&L))," October 7, 2011, http://www.acq.osd.mil/docs/Acting%20USD%28ATL%29%20Initial%20Guidance%20Memo.pdf

Under CSIAC we will continue to seek the addition of new data and new types of data as well as expand the database to include systems and systems-of-systems data. We recently formalized a partnership with the Australian Defence Materiel Organisation to enhance the breadth and variety of software and systems data, as well as expanding its use across our global partners.

CSIAC to Create a Community of Practice for the Cyber Security and Information Systems Community

Our strategy for the CSIAC is to build and facilitate a "Community of Practice (CoP)" to address the broadened scopes of the three IACs (DACS, IATAC, MSIAC), as well as the new areas of Knowledge Management and Information Sharing. Many of you have been members of the DACS or IATAC LinkedIn discussion groups and have thus been part of the DACS and IATAC community of practice already.

The newly established CSIAC website (www.thecsiac.com) serves as a catalyst for the CSIAC CoP, as well as providing its infrastructure. The CSIAC CoP is a member driven website that encourages participation from the CSIAC community supported by CSIAC resources and activities. The emphasis is on unifying CSIAC resources and members around the concept of conversations and collaboration. These conversations and the high-level conceptual framework are supported by open source and semantic web tools. The values of participation, learning, members, and conversation are based on concepts out of information science and learning theory that emphasize participation and social interaction. The CoP is a powerful concept for gaining and sharing knowledge in the CSIAC user community through interaction and discussion. It is through this discussion, sharing information and experiences within the group, that users learn from each other. The CoP will support the entire operation of the CSIAC, including information collection, analysis, and dissemination.

The new CSIAC provides distinct advantages and value added to our users:

- Community expertise, knowledge and discussion becomes a new dimension and benefit for CSIAC users
- Users will be able to draw directly from practitioners and other experts when needed to answer their urgent questions
- Users will be able to identify true subject matter experts (SMEs) based on community recommendations, and can follow SME contributions using typical social networking "recognition" techniques
- CSIAC and CSIAC users will be able to gain access to additional scientific and technical information – not just formal reports and documentation, but live, interactive, and tailored knowledge from an active community of experts
- Collaboration capabilities of the CoP will allow the CSIAC user community to create products, such as best practice documents, as well as encourage community support of products developed
- The CoP will provide opportunities for users to contribute their unique knowledge and experience, enhancing the breadth, depth, and relevance of the CoP
- Users will be able to provide feedback to CSIAC on current offerings, and recommendations for the future

We welcome your input on what the CSIAC is doing, how it could be better, and suggestions for new CSIAC activities. Feel free to contact me at: Christopher.j.zember@dtic.mil or you can email your comments to the CSIAC Director directly at: tmcgibbon@quanterion.com. We thank you in advance for your partnership as we adapt to the evolving needs of you, our community.

About the Authors

Christopher Zember is the Deputy Director of the DoD IACs, under oversight of the Assistant Secretary of Defense for Research and Engineering. He is responsible for operational management and policy guidance for 10 IACs, comprising a $14 billion portfolio in technical research and analysis. Prior to his current position, Mr. Zember led the Strategy and Operations practice for a small consulting firm and also served as a member of the core research team in a congressionally-chartered effort to rewrite the National Security Act. Mr. Zember holds a B.A. in English from Harding University and a M.P.A. from American University.

Thomas McGibbon works for Quanterion Solutions, Inc. as the Director of the CSIAC. He has over 30 years of experience in software development, systems development, and software project management. He is author of several DACS state of the art reports on software engineering topics. He holds a MS in Software Engineering from Southern Methodist University and BS in Mathematics from Clarkson University.

Cyber Security… The Virtual Frontier

By Paul M. Engelhart, CSIAC Contracting Officer's Representative (COR)
Air Force Research Laboratory - Rome Research Site

Just a few short months ago on July 1st, 2012 the new Cyber Security and Information Systems Information Analysis Center (CSIAC) contract was awarded to Quanterion Solutions Incorporated, marking the beginning of a new era within the Defense Technical Information Center (DTIC) Information Analysis Center (IAC) program as the first combined Basic Center Operation (BCO) contract. Formed as the consolidation of three legacy IAC's – the Data and Analysis Center for Software (DACS), the Information Assurance Technology Assurance Center (IATAC), and the Modeling and Simulation Information Analysis Center (MSIAC) – along with the addition of the new technical domain of Knowledge Management and Information Sharing, the CSIAC is chartered to leverage best practices and expertise from government, industry, and academia on cyber security and information technology. Operating in an agile manner, the CSIAC will monitor and utilize emerging technologies of information assurance, software technology, software and systems engineering, modeling and simulation, knowledge management and information sharing.

As discussed in the Information Analysis Center Strategic Plan for 2010-2015, the overarching vision of the IAC program is based on driving innovation and technological developments by successfully anticipating, as well as responding to, the information needs of the defense user community while enhancing collaboration through integrated Scientific and Technical Information (STI) development and dissemination. However, increased access to information presents both challenges as well as opportunities. The speed of information allows us to connect resources in real-time, but our adversaries have achieved that same benefit. In the past, we have been faced with limited access to information. Our current challenge is sorting through too much data to find the right information for the right person at the right time. The CSIAC is poised, through the implementation of their innovative Community of Practice collaboration concept, to provide unbiased STI and analysis, based on collecting resources from around the world and across time, in order to provide timely, relevant and accurate information.

As we look into the near and distant future, it reminds me of the original Star Trek vision back in the mid-60's: "Cyber security… the virtual frontier. These are the voyages of the Cyber Security and Information Systems Information Analysis Center. It's continuing mission… to explore strange new challenges, to seek out new technologies and new paradigms, to boldly go where no one has gone before." As we forge ahead with the new CSIAC, please feel free to contact us with any feedback, concerns, and/or questions. The CSIAC is here to help you!

About the Author

Paul M. Engelhart is a Senior Computer Engineer at the Air Force Research Laboratory/ Information Directorate – Rome Research Site. He has over 31 years of experience in the software engineering field, including 19 years as the DACS COR prior to the formulation of CSIAC. Mr. Engelhart holds a Bachelor of Science degree in both Mathematics and Computer Science from the State University of New York at Cortland and a Master of Science degree in System and Information Sciences from Syracuse University. He can be contacted at Paul.Engelhart@rl.af.mil

Signcryption for Biometric Security

By Phillip H. Griffin, CISM

Biometrics is the "something you are" identity factor used in authentication and identification systems. Organizations that rely on biometric technology should ensure the confidentiality, integrity and authenticity of their biometric assets. To manage security risk, biometric information should be protected from unauthorized access and modification.

Biometric assets should be protected while at rest and during transfer, both within the firewall perimeter and across public networks such as the internet. A signcryption cryptographic operation protects information with a digital signature and encryption. Signcryption can be used to manage security risk and to provide assurance of the confidentiality, integrity and authenticity of biometric information.

Signcryption is a relatively new cryptographic primitive, standardized last year as ISO/IEC 29150 [1]. Signcryption uses "an asymmetric encryption scheme and a digital signature scheme combined in a specific way", along with "a specially developed algorithm" [1] to perform both encryption and digital signature functions simultaneously. This efficient cryptographic technique provides data integrity, origin authentication, and data confidentiality in a single operation.

Hybrid Cryptographic Primitives

The signcryption primitive is a hybrid cryptographic primitive. Hybrid cryptography is that "branch of asymmetric cryptography that makes use of convenient symmetric techniques to remove some of the problems inherent in normal asymmetric cryptosystems". These problems include those encountered securing large iris scan, DNA, or fingerprint sets that require systems "to process long messages quickly" [2].

Though signcryption was only approved recently as an international security standard, hybrid cryptography is not a new technology. Authenticated encryption is a family of familiar hybrid cryptographic techniques commonly used to secure network communications. These techniques use "a shared-key based transform" that relies on a symmetric encryption scheme "to provide both privacy and integrity" [3]. Signcryption can be considered the asymmetric analog of authenticated encryption.

The Transport Layer of the Secure Shell protocol (SSH), some versions of the Secure Sockets Layer (SSL) protocol, and the Encapsulating Security Payload (ESP) protocol are all based on authenticated encryption methods. These protocols use the "Encrypt-and-MAC (E&M)", "MAC-then-encrypt (MtE)", and "Encrypt-then-MAC (EtM)" [3] authenticated encryption methods to "provide privacy and reliability" [4] services or "confidentiality, data origin authentication", and connectionless integrity [5].

These hybrid cryptographic methods are based on symmetric key encryption. Since "symmetric encryption schemes and MAC algorithms" rely on shared key, symmetric approaches to provide their security services, non-repudiation is not possible [2]. Since signcryption uses an asymmetric approach, several signcryption schemes can provide non-repudiation. However, until recently no standardized signcryption message schema could be used to manage biometric information security and protect biometric data.

Protecting Biometrics

This past April, a new signcryption message schema and processing protocol was presented to the ID360 Global Forum on Identity at the Center for Identity at the University of Texas, Austin. In a poster session, Protecting Biometrics Using Signcryption [6], a signcryption cryptographic message schema was defined. Three modes of processing were described, including one to support signcryption of selected components of a biometric transaction or reference template. The paper proposed standardization of a new cryptographic message type, named SigncryptedData, to be included as a part of the X9.73 Cryptographic Message Syntax (CMS) [7] standard.

Type `SigncryptedData` is derived from the `SignedData` type currently used to secure electronic mail, and biometric reference templates, Type-98 records in ANSI/NIST ITL [9] and DoD EBTS biometric transactions. The `SignedData` type is also used to manage biometric

information and security in the X9.84 and ISO 19092[1] biometric security standards.

The X9.84 biometric information management and security standard describes how messages containing biometric information can be bound cryptographically to a set of security and other metadata attributes [10].

This binding under a digital signature in a `SignedData` message wrapper provides origin authenticity and data integrity, and binds biometric data to security management information, such as Need-To-Know (NTK), Information Security Marking (ISM), and Geospatial Intelligence (GEOINT) information. Without the protection of a digital signature, accidental and malicious changes to data can go undetected, and data integrity cannot be assured.

The increased need for sharing biometric information among law enforcement, defense, and intelligence agencies has made origin authenticity of biometric information crucial for organizations that share biometrics. Decisions based on the accuracy and reliability of biometric information can affect National Security. It is crucial that decision makers receive biometric information that is free from tampering and that has originated from a trusted source. Biometric data and associated security metadata must be protected from removal and malicious or accidental modification.

Digital signatures alone do not provide biometric data confidentiality. X9.84 requires that the biometric data elements in an information object, such as a biometric reference template or a DoD EBTS transaction, be kept confidential to prevent unauthorized access and to ensure the privacy of individuals. The proposed `SigncryptedData` type extends the security protection of the SignedData message type to provide assurance of the confidentiality, data integrity, and origin authenticity of biometric information.

Implementation

A secure signcryption message can be implemented in both XML markup and a compact binary format using a single schema defined in the U.S. national standard, X9.73, and the recently proposed `SigncryptedData` type. Any type of biometric information in any format can be protected by a signature and encryption using the `SigncryptedData` cryptographic type. The protected content could be objects

1 The ISO 19092:2008 Biometrics Security Framework was derived from the ANSI X9.84 standard.

WHAT IS DOD EBTS?

The Department of Defense (DoD) Electronic Biometric Transmission Specification (EBTS) [8] was developed by the Biometrics Identity Management Agency (BIMA) to transport and store biometric data and associated DoD-relevant information. This information is transferred from biometric collection devices to a BIMA storage, matching, and distribution point. Biometric matching services are provided by BIMA to the DoD and its information-sharing partners using ABIS, the Automated Biometric Identification System.

ABIS is a central biometric storage and matching engine that responds to DoD EBTS match request transactions. ABIS sends biometric matching results and distributes biometric and associated information. ABIS transactions can be used to exchange information in one of several traditional formats, or in an Extensible Markup Language (XML) format. The DoD EBTS XML schema can support fast, efficient transactions using an analogous Abstract Syntax Notation One (ASN.1) schema that can transfer and exchange information in both compact binary and XML markup formats.

The latest version, DoD EBTS 3.0, was published as an emerging standard in 2011. It is based on the American National Standards Institute/National Institute of Standards and Technology (ANSI/NIST) Information Technology Lab (ITL) standard [9]. ITL and DoD EBTS transactions are not signed objects. These standards rely on an optional ITL Type-98 Information Assurance record to protect selected content in environments where use of the record is mandated. Best ITL guidance calls for the Type-98 record to contain a SignedData message, such as the version defined in the X9.73 CMS standard [7].

currently protected using the `SignedData` type, such as a DoD EBTS transaction, a biometric reference template, a Biometric Enabled Watch List (BEWL), or an X9.84 biometric system event journal.

The `SigncryptedData` type can be used to sign and encrypt an entire biometric object, or only specific components of the object, such as those components that should be kept confidential. Three processing modes for the `SigncryptedData` type have been proposed. These modes are identified as *signcrypted-content, signcrypted-attributes,* and *signcrypted-components*. In the s*igncrypted-content* mode, biometric data of any type is signcrypted. In the *signcrypted-attributes* mode, biometric data and associated attributes of any type are signcrypted. In the *signcrypted-components* mode, one or more components of the biometric data is signcrypted, then the resulting object is bound to one or more attributes under a digital signature.

Of these three modes, the *signcrypted-components* mode holds the most promise for protecting biometric information and associated security metadata attributes. This mode allows a biometric object containing signcrypted components to be cryptographically bound together with a set of security attributes using a digital signature. Signature processing follows the processing requirements for the X9.73 `SignedData`[2] type.

One attribute must contain a manifest, a list of the signcrypted components in the initial biometric object. This manifest must be included in the signed attributes, to ensure they are bound to the biometric object under a digital signature and available to the intended message recipient. The format and information contained in the manifest varies with the type of biometric object. For XML instance documents, such as BEWL or DoD EBTS transactions, XML Path (XPath) expressions can be used to locate the signcrypted elements. A list of XPath expressions forms a manifest that identifies the location of each signcrypted element in the biometric object.

A recipient of a `SigncryptedData` message uses the manifest to locate the elements in the XML instance document that contain signcrypted data. The signature on each signcrypted element in the list can then be verified and its plaintext content can be decrypted and recovered. Recovered plaintext can then be used to reconstruct the original XML document prior to XML schema validation.

Conclusion

Biometric information objects may carry personally identifiable information (PII). Some objects, such as DoD EBTS transactions, may be used to identify suspected terrorists or criminals; individuals that may be anonymous or whose identities are known. In some jurisdictions where information must be shared, biometric data and other PII data may be subject to laws that require privacy protection when this information can identify an individual.

In law enforcement, defense and intelligence environments, other information, such as the geolocation of an event or encounter, may be classified. Access to this information may be restricted based on a security classification level or need-to-know basis. Selected components in a message can be protected using signcryption to ensure that any sensitive information remains confidential. The biometric information object as a whole can be cryptographically bound together, perhaps with a set of security metadata, under a digital signature to give the object integrity and origin authenticity.

Signcryption cryptographic safeguards can protect the confidentiality, integrity, and authenticity of biometric information at rest, and as it travels across unprotected networks, such as the Internet. Other hybrid cryptographic techniques, such as authenticated encryption, have proven themselves as reliable cryptographic safeguards in network security protocols such as IPSec, SSH, and SSL. Signcryption is the asymmetric key analog of authenticated encryption that provides a way to integrate digital signatures with encryption schemes into a single, efficient cryptographic function. A recently proposed `SigncryptedData` cryptographic message type can be used to protect biometric information assets, such as DoD EBTS transactions, biometric watch lists, biometric reference templates, and biometric system event journals.

2 When there are attributes in type `SignedData`, the `messageDigest` and `contentType` attributes are required.

This article presents some research and study results and the author's description of them. The opinions expressed here do not necessarily represent the opinions of the DoD, BIMA, or Booz | Allen | Hamilton.

About the Author

Phillip H. Griffin, CISM | is an Associate at Booz | Allen | Hamilton serving as a subject matter expert for the Biometrics Identity Management Agency (BIMA). At BIMA, he is responsible for National Information Exchange Model (NIEM) packaging of their DoD Electronic Biometric Transmission Specification (EBTS). He has served as editor of the X9.84 and ISO 19092 biometric information management and security standards, cofounded and chaired the OASIS XML Common Biometric Format (XCBF) and OASIS Security Standards Joint Committees, and currently represents BIMA on the OASIS Biometric Identity Assurance Specification (BIAS) committee. Mr. Griffin has over 15 years experience in the development of information assurance and security standards and secure message protocols. He can be contacted at ***phil@phillipgriffin.com.***

References

1. International Organization for Standardization / International Electrotechnical Commission. (2011). ISO/IEC 29150 Information technology - Security techniques - Signcryption.

2. Dent, Alexander W. (2004). Hybrid cryptography, Cryptology ePrint Archive Report 2004/210. Retrieved July 21, 2012, from http://www.signcryption.org/publications/pdffiles/Dent-survey-eprint-04-210.pdf

3. Bellare, M., & Namprempre, C. (2008). Authenticated Encryption: Relations among Notions and Analysis of the Generic Composition Paradigm. *Journal of Cryptology*, *21*(4), 469-491. doi:10.1007/s00145-008-9026-x. Retrieved July 21, 2012, from International Security & Counter Terrorism Reference Center database.

4. Freier, A., Karlton, P., & Kocher, P. (1996). *The SSL protocol version 3.0*. Retrieved July 21, 2012, from http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt

5. Kent, S. (2005). *IP encapsulating security payload (ESP)*. Retrieved July 21, 2012, from http://ietfreport.isoc.org/rfc/rfc4303.txt

6. Griffin, Phillip H. (2012). *Using Signcryption To Protect Biometric Information*. ID360: The Global Forum on Identity, The Center for Identity, University of Texas at Austin. Retrieved July 21, 2012, from http://phillipgriffin.com/innovation.htm#ID360

7. X9 Financial Services. (2010). *ANSI X9.73:2010 Cryptographic Message Syntax - ASN.1 and XML*. U.S.A.: American National Standards Institute (ANSI).

8. BIMA. (2011). Electronic Biometric Transmission Specification (EBTS). Retrieved June 21, 2012, from http://www.biometrics.dod.mil/Files/Documents/Standards/DoD_EBTS_v3_0.pdf

9. ANSI/NIST-ITL 1-2011, NIST Special Publication 500-290, Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information. [IEPD]. Retrieved June 12, 2012, from http://www.nist.gov/itl/iad/ig/ansi_standard.cfm

10. X9 Financial Services. (2010). *ANSI X9.84:2010 Biometric Information Management and Security*. U.S.A.: American National Standards Institute (ANSI).

Securing Systems through Software Reliability Engineering

By Taz Daughtrey

Once upon a time, a brave knight was entrusted with the guarding of a valuable treasure. An evil wizard had designs on the treasure. It wasn't known what mischief was planned or exactly what form the wizard might take. Would the villain try to seize and carry away the treasure? Or simply damage or destroy it? And how would the protector recognize the wizard or detect any evil-doings?

The knight considered many possible defenses: locking the treasure in a secure chamber, surrounding it with additional barriers and guardians, even casting a magic protective spell over it. As for anticipating the wizard's attack, the knight realized that the best approach would be to try thinking like a villain -- imagining how an evil-doer might behave.

Unfortunately, there is no "happily ever after" ending to this story, for as soon as the guardian thwarted one wizard's advances another, more clever and subtle adversary arose … and the task was shown to be unending.

Is that your story, too? Securing systems from threats … threats from unknown and unseen adversaries … threats to confidentiality, integrity, or availability of systems and the information they contain. And are there tools to help you, the protector?

Software reliability engineering represents a well-established set of techniques supporting specification and assessment of dependability aspects of software-based systems. Application of these techniques to security concerns could provide helpful assistance for software assurance efforts.

Software reliability is defined as "*the ability of a program to perform a required function under stated conditions for a stated period of time*." Quantitatively, this may be considered as "*the probability that software will not cause the failure of a system for a specified time under specified conditions.*" [1]

Reliable software does what it is supposed to do. Unreliable software fails to meet expectations, but may do so in any of a number of ways. An unreliable software-based system may be unavailable, incorrect, vulnerable, or possibly even unsafe. This variety of inadequacies and failure modes includes both "sins of omission" (not behaving as intended) and also "sins of commission" (behaving in unintended ways).

A system in failure mode may be characterized by degraded performance, unexpected behavior, or complete loss of functionality. The severity with which the failure is regarded depends on the type of mission itself. What is the nature of our dependency on a given system? Failures of business-critical systems frustrate the accomplishment of their entrusted business function. Systems handling sensitive personal or financial information can have security-breaching failure modes. Failures of safety-critical systems imperil safety.

Software unreliability may arise from errors such as specifying incomplete, ambiguous, or conflicting requirements; from inappropriate design choices; from incorrect implementation; or from any number of other opportunities for mistakes throughout the development process. These defects may often be subtle and very difficult to locate, given software's complexity and immateriality

John Musa [2] championed software reliability engineering (SRE) as a systematic and data-driven means for achieving desired levels of reliability. SRE represents "the application of statistical techniques to data collected during system development and operation to specify, predict, estimate, and assess the reliability of software-based systems."

The classic Plan-Do-Check-Act cycle may be seen in the overarching approach of SRE:

Plan addresses setting reliability targets in measureable terms ("*specify and predict*").

Do is the design and implementation of the system with those expectations.

Check represents all the appraisal activities up through system-level testing ("*estimate and assess*").

Act then closes the loop and may lead to rework of the product or even retargeting of reliability goals.

At each stage of software development, available data are gathered and analyzed. The resulting reliability estimates then support data-based management decisions (See Figure 1).

Stage	Data Available	Analysis Supports
Planning	Organizational Process Maturity Project Histories	Feasibility of Reliability Targets
Development	Appraisal Reports	Rework
Testing	Test Failure Data	Rework Release Decision
In Use	User Feedback Field Failure Data	Repair or Recall Improving Next Development

Figure 1. Lifecycle Software Reliability Measurements

At the planning stages of a project one may draw upon historical data from similar previously developed systems (including operational performance) as well as the organization's assessed process maturity. Throughout development, defect detection provides opportunities for rework that can improve the final product. The timing of failures encountered in testing has been used to model projected operational reliability. Ideally SRE can support data-driven project decisions, most significantly the decision of when to release a product that is under development.

Consider that some of the most significant aspects of SRE include:

establishing quantitative reliability targets,

constructing usage profiles of the operational system, and

conducting statistically based testing to predict system reliability.

By analogy, security analysis could apply a similar approach with suitable modifications, such as:

establishing quantitative security targets including availability and loss function,

using threat modeling to identify a variety of misuse/abuse cases, and

rethinking reliability growth modeling in terms of security growth modeling.

Software security engineering would utilize activities across the development life cycle including:

- *Initiation Phase* of preliminary risk analysis, incorporating history of previous attacks on similar systems.
- *Requirements Phase* establishing appraisal management processes and conducting more detailed risk analysis.
- *Design Phase* focusing resources on specific modules, such as those designed to provide risk mitigation.
- *Coding Phase* with functional testing to begin at the unit level as individual modules are implemented.
- *Testing Phase* moving from unit testing through integration testing to complete system testing.
- *Operational Phase* requiring attention as deployment may involve configuration errors or encounters with unexpected aspects of the operational environment.

Reliability analysis has historically had to consider only failures due to accidental encounters with pre-existing software defects. However, security concerns arise from active attempts to exploit system weaknesses – some of which may have been deliberately inserted by the same or other villains.

The subset of defects that might be exploited to breach security is typically referred to as *vulnerabilities*. Taking advantage of these weaknesses could adversely affect confidentiality, integrity, or accessibility of a system or its data.

The lower left quadrant in Figure 2 represents the realm that traditional reliability efforts have addressed: locating and removing defects inadvertently introduced into a system during its development or maintenance. However, users are now encountering other situations, as represented in the upper left quadrant. Some issues result from design or implementation tradeoffs in which potentially conflicting requirements (such as maximizing both efficiency and usability) have been satisfied through sub-optimizing one or both. More troublingly, the topmost region of the upper left quadrant represents malicious acts such as the installation of back doors, trojans, or other deliberate weaknesses in the system. Someone with a knowledge of these weakness could then purposefully seek to exploit them, as shown in Figure 3.

Such malicious behavior also makes it more complicated to estimate the probability of system failure. A successful attack depends on a sequential set of factors in terms of knowledge, skills, resources, and motivation:

What is the attacker's *knowledge* about existing vulnerabilities?

How likely is an attacker to possess the *skills* required to exploit a known vulnerability?

How extensive are the *resources* (access, computing power, etc.) that the attacker might bring to bear?

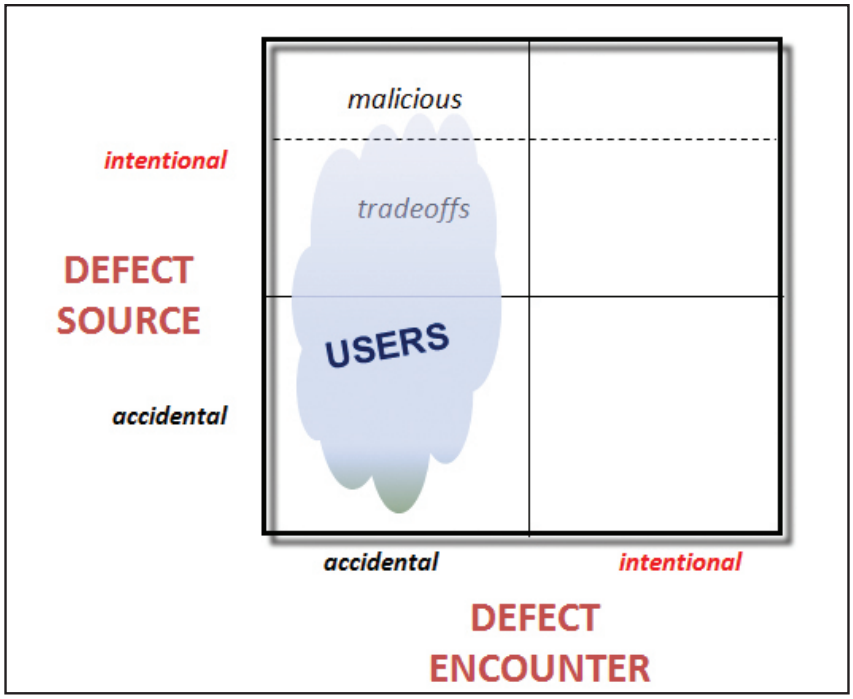


Figure 2. Distribution of Use

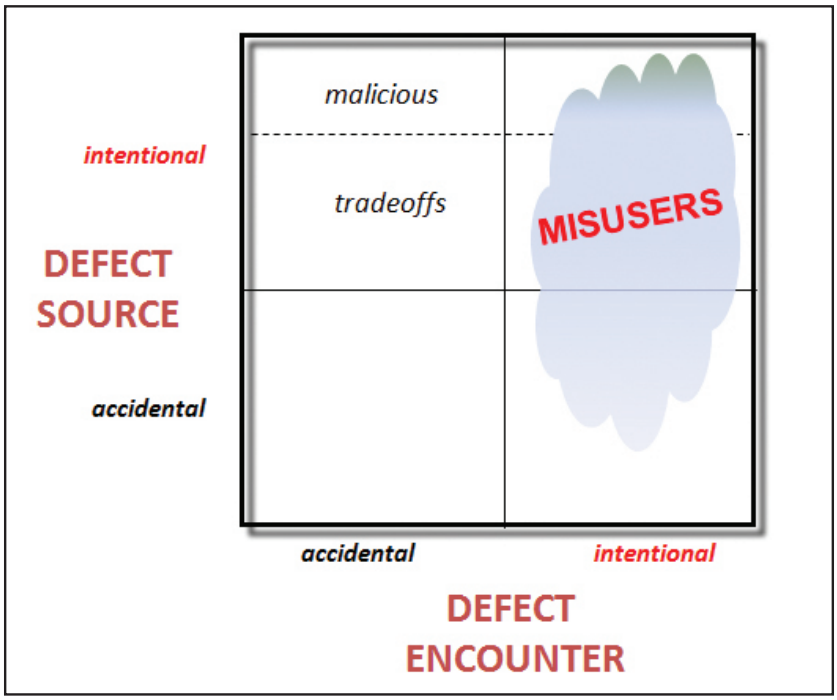


Figure 3. Distribution of Misuse

What *motivations* would keep a given attacker on task to successful completion of the attack?

Thus, a multiplicative series of probabilities must be considered. Threat modeling explores a range of possible attackers, all with different capabilities and incentives, and profiles these characteristics. Identifying potential threats to security is inherently more complex and uncertain than working within a well-defined community of stakeholders, all of whom wish the system to work successfully. First, the value of the system – its appeal to attackers – must be characterized across a range of potential misusers. Further, different attackers will themselves have different definitions of success, such as the extent to which they wish to remain undetected or anonymous.

Just as traditional usability and reliability assurance need a proper context for their design and interpretation, so too security assurance needs its own context if it is to provide useful insights. Threat modeling can be considered analogous to the development of operational profiles in reliability testing. Rather than being driven by customer- or user-supplied requirements, security assurance is typically mapped against anticipated attacks on the system. Hence the development of *misuse* (or *abuse*) *cases* to describe conditions under which attackers might threaten the system, in contrast to the traditional use cases, which describe "normal" interaction pattern.

Security assurance activities also require special attention. For instance, results of tests need to be considered with more nuance than simply noting whether or not security was compromised. They must be calibrated in terms of cumulative success factors:

- What *knowledge* about a given vulnerability was assumed in the test case?
- What specific *skills* and skill levels were employed within the test?
- How extensive were the *resources* that were required to execute the test?
- What *motivations* of an attacker would be sufficient to persist and produce a similar result?

Security growth modeling, analogous to reliability growth modeling, is an attempt to quantify how the projected security of a system increases with additional detection and removal of software vulnerabilities. Such insights would be crucial in allocating development and assurance resources, as well as making informed release or revision decisions. Security growth modeling relies on several analytical processes beyond those in traditional reliability growth modeling, including threat modeling.

The quantification of absolute security risk remains a long-range (if possibly unattainable) goal, but the approach described should allow for better understanding of relative risks and of the expected ROI from reduction of security risk exposure. The quest continues.

[Versions of this material were presented in a DACS webinar in August 2011 (http://www.thedacs.com/training/webinar/poll/index.php?pid=353) and at the Software Engineering Process Group – North America conference in March 2012. My thanks to the reviewers and facilitators at those events.]

End Notes

1. Institute of Electrical and Electronics Engineers. 2008. IEEE Std 1633-2008, IEEE Recommended Practice on Software Reliability.

2. Musa, John. 2005. "Software Reliability Engineering: Making Solid Progress." SOFTWARE QUALITY PROFESSIONAL. Vol. 7, No. 4, pp 5-16.

About the Author

Taz Daughtrey (daughtht@jmu.edu) is Senior Software Quality Scientist at Quanterion Solutions and a member of the Computer Science faculty at James Madison University . He is a Fellow of the American Society for Quality, the Founding Editor of the journal SOFTWARE QUALITY PROFESSIONAL, and a director on the American Software Testing Qualifications Board. Taz's previous industry responsibilities included serving as corporate Quality Manager and Chief Security Officer, as well as roles in software development, training, and quality improvement in commercial and naval nuclear engineering and manufacturing.

Shaping Preventive Policy in "Cyber War" and Cyber Security: A Pragmatic Approach

By Tony S. Guo

On January 28th, 2011, Egypt disappeared from the global map. In a coordinated shutdown of all major Egyptian internet service providers--an effort by its government to squelch public dissent--virtually all Egyptian Internet addresses became unreachable worldwide.[1] The action was unprecedented in Internet history.[2] At the same time, the U.S. Senate introduced a bill that would give the President the same power to shutdown "critical" Internet infrastructure in the event of a "national cyber emergency."[3] This bill and others like it were introduced in light of the political rhetoric on "cyber war."

In recent years, "cyber war" has emerged as one of the nation's most widely publicized national-security concerns. "In the past, you would count the number of bombers and the number of tanks your enemy had. In the case of cyber war, you really can't tell whether the enemy has good weapons until the enemy uses them," says Richard Clarke, former chairman of the White House Critical Infrastructure Protection Board.[4] In his recent book, *Cyber War*,[5] Clarke forecasted that an offensive cyber war on the United States might result in the following:

> Within a quarter hour, 157 major metropolitan areas have been thrown into knots by a nationwide power blackout hitting during rush hour. Poison gas clouds are wafting toward Wilmington and Houston. Refineries are burning up oil supplies in several cities. Subways have crashed . . . [f]reight trains have derailed . . . [and] [a]ircraft are literally falling out of the sky as a result of midair collisions across the country. . . . The financial system has also frozen solid . . . . Several thousand Americans have already died.[6]

Former Vice-Admiral John Michael McConnell echoed similar warnings, stating that "the United States is fighting a cyber war today, and we are losing" because "our cyber-defenses are woefully lacking" and "we have not made the national commitment to understanding and securing cyberspace."[7]

Clarke is currently a Managing Partner at Good Harbor Consulting, a firm that advises governments and companies on cyber security and other issues.[8] McConnell is now Vice Chairman of Booz Allen Hamilton, a defense contractor that recently landed a $34 million cyber contract, $14.4 million of which was required to build the recently completed United States Cyber Command (CYBERCOM).[9] CYBERCOM was officially activated on May 21, 2010 and announced its first commander, Army General Keith Alexander,[10] who made it clear that he wants more access to e-mails, social networks, and the Internet in order to protect America and fight in what he sees as the new warfare domain, cyberspace.[11] The federal government currently spends $6-7 billion annually on

1 *See* Ryan Singel, *Egypt Shut Down Its Net With a Series of Phone Calls,* Wired, Jan. 28, 2010, *available at* http://www.wired.com/threatlevel/2011/01/egypt-isp-shutdown/.

2 *See Id.*

3 S. 3480, 111th Cong. (2009), *available at* http://www.govtrack.us/congress/bill.xpd?bill=s111-773. Strangely enough, this bill actually purports to "limit" the President's existing power to shut down Internet infrastructure under Section 706 of the Communications Act of 1934. *See infra* Section V(A). The bill ultimately failed

4 *See* frontline: cyberwar!: introduction | PBS, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/etc/synopsis.html (last visited Nov. 7, 2011).

5 Richard A. Clarke, Cyber War 67 (HarperCollins 2010).

6 *Id*. at 67.

7 *See* J. Nicolas Hoover, *Former Intelligence Chief: U.S. Would Lose Cyberwar*, InformationWeek, Feb. 23, 2010, *available at* http://www.informationweek.com/news/government/security/showArticle.jhtml?articleID=223100425.

8 *See* Richard A. Clarke – Partner, Good Harbor Consulting, http://www.goodharbor.net/team/clarke.php (last visited Nov. 12, 2010).

9 *See* John M. McConnell – Executive Vice President, Booz, Allen, & Hamilton, http://www.boozallen.com/about/leadership/executive-leadership/McConnell (last visited Nov. 12, 2010). *See also* Ryan Singel, *Cyberwar Doomsayer Lands $34 Million in Government Cyberwar Contracts,* Wired, Apr. 13, 2010, *available at* http://www.wired.com/threatlevel/2010/04/booz-allen/.

10 *See* DOD Announces First U.S. Cyber Command and First U.S. CYBERCOM Commander, U.S. Defense Department, May 21, 2010, http://www.defense.gov/releases/release.aspx?releaseid=13551.

11 *See also* Seymour Hersh, *The Online Threat,* The New Yorker, Nov. 1, 2010, *available at* http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

unclassified cyber security work, and pundits have criticized that Clarke, McConnell, and others have been using the national limelight to create what has become a military-cyber complex.[12]

The recent proponents of "cyber war" may have profitable motives, and there is no evidentiary basis that cyber *warfare* has ever been waged, or will be in the immediate future. However, American security officials for the most part agree that cyber security is highly relevant to national security, and it is theoretically possible that a foreign military or an independent hacker could be capable of creating a degree of chaos in the United States.[13] These fears, however, may have been exaggerated. Some argue that the confusion in terminology has led to a belief that cyber war is *already* here, and the real danger lies in the difficulties of holding the military back from infringing on our civil liberties.[14]

This article attempts to provide a cogent analysis of "cyber war," cyber security, and preventive policy. It argues that "cyber war" is not "war," and the laws of warfare do not apply. Cyber war is an issue of security--systems security, network security, and due diligence on part of its operators--the legal responses considered should be limited to such. Part I will draw distinctions in cyber security, specifically between attempted definitions of "cyber war," cyber espionage, and related terminology. Part II will explain the difficulties of applying law on warfare as a deterrent, and why "cyber war" should not be considered as war. Part III argues that "cyber war" is an exaggerated hypothetical, and most security breaches today are issues of poor systems security and human error. Lastly, Part IV outlines some past and present legal responses, and what they might mean to all Internet users in the future.

I. Definitions and Terminology

John Keegan, in *A History of Warfare*, stated that "war" is a "universal phenomenon whose form and scope is defined by the society that wages it."[15] If war is an evolving concept with no set definition, then how do we define cyberwar? Does it even exist? Despite the attention on the defense departments over cyber security in recent years,[16] an entry for the term "cyberwar" is still missing from the Department of Defense's Dictionary of Military and Associated Terms.[17] Although an official definition is missing, several others exist.

In Clarke's book, *Cyber War*, cyberwarfare is carefully defined as "actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption."[18] The Economist has coined cyberwar as "war in the fifth domain," and as a doctrinal matter, the Pentagon has "formally recognized cyberspace as a new domain of warfare . . . just as critical to military operations as land, sea, air, and space."[19]

A concrete definition is important for legal consequences. For instance, a cyber attack that hacks into a corporate website and defames it is not an act of war, domestic criminal laws would apply, and full Constitutional rights would be enforced. On the other hand, a cyber attack with real, physical repercussions, such as blowing up an oil pipeline, is a use of force, and the perpetrators might be dealt with as enemy combatants.[20]

Richard Clarke's definition of cyber war does not make war sound so bad: an act by one nation-state to penetrate another's networks for purposes of causing damage or disruption. Under this definition, a single act by a foreign national--assuming it could be attributed to that state--to defame the United States Parks and Recreation website would be for all purposes, an act of war.

Despite war being an evolving concept, in most of our minds it elicits images of the beachfront of Normandy, of kinetic weapons, loud explosions, mushroom clouds, and a

12 Seymour Hersh, *The Online Threat,* The New Yorker, Nov. 1, 2010, *available at* http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

13 *See Id.*

14 *See Id.*

15 John Keegan, A History Of Warfare, (Pimlico 1994)

16 *See,* e.g., Cyberwar – Series – The New York Times, http://topics.nytimes.com/topics/features/timestopics/series/cyberwar/index.html (last visited Dec. 18, 2010); front line: cyberwar! | PBS, http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar (last visited Dec. 18, 2010).

17 *See* DOD Dictionary of Military and Associated Terms, http://www.dtic.mil/doctrine/dod_dictionary/ (last visited June 16, 2012).

18 Richard A. Clarke, Cyber War 6 (HarperCollins 2010).

19 *See* William J. Lynn III, *Defending a New Domain,* Foreign Affairs, Sept. 2010, available at http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain.

20 Whether the perpetrator would be classified as an enemy combatant would also depend on citizenship, the locus of capture, and the place of detention. *See, e.g.,* Rumsfeld v. Padilla, 524 U.S. 426 (2004), Boumedine v. Bush, 553 U.S. 723 (2008), Hamdan v. Rumsfeld (2006), 548 U.S. 557, and Al-Marri v. Pucciarelli, 543 F.3d 213 (2008).

high degree of mortality. Today, the term "cyber war" has been thrown around loosely in the media. It has been a catch-all phrase, used to refer to everything from purely financial crimes to network attacks with physical manifestations that could kill people.[21]

Scott Charney, Microsoft's Vice President of Security, has proposed to categorically separate different cyber threats, so governments and organizations are able to think and respond differently to varying degrees and types of cyber attacks. He named three distinct areas, not to be confused with cyber war: (1) conventional cyber crimes - cases where computers are targeted for traditional criminal purposes, i.e. financial fraud; (2) military espionage - allegations that one nation-state intrudes into and captures sensitive military data of another; and (3) economic espionage – one nation's support or failure to condemn its indigenous industries from stealing the intellectual property of another nation-state.[22]

A fourth category, or perhaps a subcategory under conventional crimes, has emerged again recently under the public eye, "hacktivism." After the arrest of WikiLeaks[23] founder Julian Assange, hacktivism was used as a form of protest. [24] From prison, Assange proclaimed that "Visa, Mastercard, PayPal, and others are instruments of US foreign policy," and soon, widespread disruption followed after a hacktivist group disseminated tools to aid in the DDoS[25] attacks on the websites of MasterCard, Visa, and PayPal.[26] 1.3 million Gawker users passwords were also compromised, and Gawker's Twitter accounts were hijacked to publish messages supporting WikiLeaks.[27]

Unlike espionage, cyber war involves the penetration of foreign networks for purpose of disrupting or dismantling those networks, and making them *inoperable*.[28] However, quantifying and attributing the threat remains a challenge. First, in quantifying the threat, what amount of damage, or what length of disruption, is required to render a network "inoperable?" Where do we draw the line to distinguish between a cybercrime, such as DDoS hacktivism, vs. cyber war? Second, what degree of attribution is required before we "go to war," in an interconnected world where any individual might remotely control thousands of other networks from a terminal anywhere in the world?

In addressing these difficulties, Charney laid out six specific factors to consider: (1) many actors; (2) many motives; (3) indistinguishable attacks; (4) shared and integrated structure; (5) unpredictable consequences; and (6) potentially disastrous impact.[29] Because the Internet is a shared and integrated domain, it would be difficult to separate military and civilian targets, and the risk of casualties to non-combatant property would be significant and hard to predict.[30] Furthermore, society today is redefining "warfare" asymmetrically, characterized by low-intensity conflicts, and a nation-state might often find itself "at war" with a single individual.[31]

Does "cyber war" exist, or is it mere fear mongering? Former White House Cybersecurity Coordinator, Richard Clarke, believes so. He believes that a cyber attack could occur at anytime, anywhere, and severely cripple the nation's infrastructure. His successor, Howard Schmidt, takes a different tone. He says that there is no cyber war, cyber warfare is a terrible metaphor, and there would be no winners in an environment where the world is so interconnected and share the same underlying domain.[32]

21 Jordan Robertson, *Experts question use of 'cyberwar' for misdeeds,* Associated Press, May 5, 2010, *available at* http://www.msnbc.msn.com/id/36969943/ns/technology_and_science-security/

22 Scott Charney, *Rethinking the Cyber Threat,* Microsoft (2009), *available at* http://go.microsoft.com/?linkid=9729572.

23 WikiLeaks is an international nonprofit organization that publishes submissions of secret, confidential, and classified documents and media from anonymous sources. *See* Wikileaks:About, http://web.archive.org/web/20080314204422/http://www.wikileaks.org/wiki/Wikileaks:About (last visited Jan. 7, 2010)

24 *See* Cahal Milmo & Nigel Morris, *Prepare for all-out cyber war,* The Independent, Dec. 14, 2010, *available at* http://www.independent.co.uk/news/media/online/prepare-for-allout-cyber-war-2159567.html.

25 Thousands of users downloaded the Distributed Denial of Service (DDoS) programs, intended to render computer resources unavailable to its users, whereby thousands of computers bombard the targeted network with so many requests that it cannot respond to legitimate traffic. *See* Intrusion Detection FAQ: Distributed Denial of Service, SANS Institute, http://www.sans.org/security-resources/idfaq/trinoo.php (last visited Jan. 10, 2011).

26 Cahal Milmo & Nigel Morris, *Prepare for all-out cyber war,* The Independent, Dec. 14, 2010, *available at* http://www.independent.co.uk/news/media/online/prepare-for-allout-cyber-war-2159567.html.

27 *Id.*

28 Seymour Hersh, *The Online Threat,* The New Yorker, Nov. 1, 2010, *available at* http://www.newyorker.com/reporting/2010/11/01/101101fa_fact_hersh.

29 Scott Charney, *Rethinking the Cyber Threat,* Microsoft (2009), *available at* http://go.microsoft.com/?linkid=9729572.

30 *See Id.*

31 *Id.*

32 Ryan Singel, *White House Cyber Czar: 'There Is No Cyberwar,'* Wired, Mar. 4, 2010, *available at* http://www.wired.com/threatlevel/2010/03/schmidt-cyberwar. *See also infra* Part III(A).

Whether cyber war exists depends on the definition we give it, but it is not simply a matter of semantics, because it determines how governments prepare and respond to various threats. It is important to keep in mind that warfare in the context of cyberspace should not be easily analogized to traditional kinetic warfare, and that existing international law does not have the foresight to encompass the asymmetrical shift towards low-intensity conflicts from a wide range of anonymous attackers inspired by unknown motives.

II. "Cyber War" is not War

Existing international laws governing warfare prohibits a state from the "threat or use of force" against another state. [33] Two exceptions exist to this prohibition: (1) actions sanctioned by the Security Council in response to a "threat to the peace, breach of the peace, or act of aggression," or (2) acts of self-defense in response to an "armed attack." [34] A typical cyber attack is unlikely to meet a threshold of "force" or "armed attack" to justify retaliatory action, and under the current internet framework, an attribution that the attack was performed by "another state" is near impossible where any actor can act from anywhere with unknown motives. The issue lies not in the law, new treaties and refined definitions will not obviate the eye-for-an-eye framework of international laws on warfare, which presupposes the clear identity of an aggressor and the defined scope of aggression.

Accurate traceability of a cyber attack is difficult, sometimes impossible, in the current Internet environment.[35] Unlike the telephone system, which required tracking and billing capabilities, the Internet was not designed for tracking or tracing the behavior of its users.[36] Originally, the Internet was designed to harbor and facilitate collaboration between communities of researchers, and the tracking of benign users was never a consideration. In fact, one of the original goals of the Internet was that the network be robust and survive in case of accidents or physical damage to the routing infrastructure. Thus, there are many alternative paths to a destination, and packets[37] are automatically rerouted when the most direct path is not available.[38]

One of the consequences of this design was the lack of authentication for individual IP packets. This means the information found within, such as the source address, can be easily spoofed.[39] For one-way communication, the attacker only needs to modify the source address, but the attack will be "blind" since the attacker is unable to see the replies sent to the spoofed address.[40] A two-way communication attack is more difficult, but still possible. The attacker has to be connected to the same local network as the spoofed source address, and can use tools to sniff the reply packets as they travel to the spoofed source from the gateway router.[41] Another way to hide the origin of an attack is to use a series of intermediate hosts, also referred to as a "packet laundering" technique.[42] By using a large number of intermediaries, this technique is very effective in thwarting trace back[43] attempts when there are significant time delays between attacker activities.[44]

Under current conditions, cyber crimes, cyber espionage, and other attacks can be directed remotely, with the perpetrator's identity and location hidden. To address this problem, former Vice-Admiral and current Vice Chairman of Booz Allen Hamilton, Michael McConnell, advocated for re-engineering the Internet:

> We need to develop an early-warning system to monitor cyberspace, identify intrusions and locate the source of attacks with a trail of evidence that can support diplomatic,

33 *See* U.N. Charter art. 2.

34 *See* U.N. Charter art. 39, 51.

35 *See* John Markoff, Internet's Anonymity Makes Cyberattack Hard to Trace, July 16, 2009, NY Times, *available at* http://www.nytimes.com/2009/07/17/technology/17cyber.html?_r=1.

36 *See* Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues*, Nov. 2002, Carnegie Mellon University, available at http://www.sei.cmu.edu/reports/02sr009.pdf [hereinafter Lipson].

37 Data is sent across networks on the Internet via IP packets, each packet contains the data to be sent, the source address, the destination address, a port number. Ports represent the type of service offered by a host machine, i.e. email, file transfer, or a website. *See* Port Numbers, IANA, http://www.iana.org/assignments/port-numbers (last visited Jan. 4, 2010).

38 *See Id*.

39 *See* Rik Farrow, Source Address Spoofing - Microsoft TechNet (last visited Jan. 5, 2011).

40 *See* IP Spoofing | Network Dictionary, http://www.networkdictionary.com/security/ipspoofing.php (last visited Jan. 4, 2011).

41 *See Id*. *See also* Spoofer Project: FAQ, http://spoofer.csail.mit.edu/faq.php (last visited Jan. 4, 2011).

42 *See* Lipson at 28.

43 Due to lack of authentication, trace back attempts are analyzed based solely on an algorithm that measures packet size and timing, thus by attacking at irregular intervals, or by sending diverse packets, the attacker throws the trace off of the attacker's "scent." *See* Lipson at 28.

44 *See Id*.

> military and legal options — and we must be able to do this in milliseconds. More specifically, we need to re-engineer the Internet to make attribution, geo-location, intelligence analysis and impact assessment — who did it, from where, why and what was the result — more manageable.[45]

McConnell further suggested that the technologies were "already available from public and private sources" and can be "further developed to build them into our systems, and into the systems of our allies and trading partners."[46] The immediate effects are clear: an undertaking would fuel billions into the military's black budget and billions more to their private contractors. Existing network technology may become obsolete, and increased transaction cost of new infrastructure will bar many private entities from market. Activity of any user can be pinpointed--what was downloaded, what might have been said, what search terms were used--in case of an "attack." The perceived dangers may have merit, must be weighed against the economic harms and infringements on civil liberties.

III. Reasonable Cyber Security

"Cyber war" today exists only in the hypothetical, and its disastrous impacts are often exaggerated. For instance, the Estonia incident is a commonly cited example by proponents of "cyber war," where a number of Estonian government websites were temporarily disabled by angry Russian citizens.[47] A crude distributed denial of service (DDoS) attack was used to temporarily keep users from viewing government websites.[48] To borrow an analogy, the attack was akin to sending an army of robots to board a bus, filling the bus so that regular riders could not get on.[49] A website would fix this the same way a bus company would, by identifying the difference between robots and humans, and preventing the robots from getting on.[50]

A following MSNBC article dressed up the Estonia incident and asked the question, could a cyber skirmish lead the U.S. to actual war?

> Imagine this scenario: Estonia, a NATO member, is cut off from the Internet by cyber attackers who besiege the country's bandwidth with a devastating denial of service attack. Then, the nation's power grid is attacked, threatening economic disruption and even causing loss of life as emergency services are overwhelmed . . . outside researchers determine the attack is being sponsored by a foreign government and being directed from a military base. Desperate and outgunned in tech resources, Estonia invokes Article 5 of the NATO Treaty -- an attack against one member nation is an attack against all.[51]

The article claimed that "half of this fictional scenario occurred in 2007." In reality, a lot less than half of it occurred, most Estonian sites immediately cut off access to international traffic soon after the increased bandwidth consumption, and botnet IP addresses were soon filtered out.[52] Most of the attackers could not be traced, but one man was later arrested and fined £830 for an attack which blocked the website of the Prime Minister's Reform Party.[53]

"Cyber war" has been a source of confusion due to the ubiquitous application of the terminology, inclusive of cyber crimes and cyber espionage. Cyber warfare comes with many faulty premises, for instance, proponents argue that it might allow terrorists to successfully attack a much larger target and do disproportionate damage.[54] However, the reality is that any sufficiently effective attack will invite disproportionate retaliation.[55] For instance, one nation may be able to make the claim that any number of nations is harboring "cyber

45 Mike McConnell, *Mike McConnell on how to win the cyber-war we're losing*, The Washington Post, Feb. 28 2010, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html.

46 *Id.*

47 *See* Estonia hit by 'Moscow cyber war', BBC News, May 17, 2007, *available at* http://news.bbc.co.uk/2/hi/europe/6665145.stm.

48 *See* Kevin Poulsen, *'Cyberwar' and Estonia's Panic Attack*, Wired, Aug. 22, 2007, available at http://www.wired.com/threatlevel/2007/08/cyber-war-and-e.

49 *See* Cyberwar Hype, Classic Liberal (Mar. 3, 2007), http://the-classic-liberal.com/cyberwar-hype.

50 *See Id.*

51 *See* Could Cyber Skirmish Lead U.S. To War?, MSNBC Red Tape Chronicles (Jun. 11, 2010), http://redtape.msnbc.com/2010/06/imagine-this-scenario-estonia-a-nato-member-is-cut-off-from-the-internet-by-cyber-attackers-who-besiege-the-countrys-bandw.html.

52 Joshua Davis, *Hackers Take Down the Most Wired Country in Europe*, Wired, Aug. 21, 2007, *available at* http://www.wired.com/politics/security/magazine/15-09/ff_estonia.

53 Estonia fines man for 'cyber war,' BBC News, Jan. 25, 2008, http://news.bbc.co.uk/2/hi/technology/7208511.stm

54 *See, i.e.,* Mortimer Zuckerman, *How to Fight and Win the Cyberwar*, The Wall Street Journal, Dec. 6, 2010, *available at* http://online.wsj.com/article/SB10001424052748703989004575652671177708124.html.

55 For example, the retaliatory attacks on Afghanistan and Iraq after the incident on September 11, 2001. *See generally* Matthew J. Morgan, The American Military After 9/11 (MacMillian 2008).

terrorists" and invoke the right of preemptory self-defense. However, "cyber war" as it exists today is not kinetic warfare and should not be confused with traditional notions of war. "Cyber war" is about how to prevent or respond to a DDoS attack, and how to secure systems and information.

Short of "re-engineering the Internet," one could simply maintain government networks and critical infrastructure on closed-networks using proprietary software or protocols. If an organization has all its systems on a closed circuit, the only threats left are its *users*. Recent data suggests that problems of attribution may not be the major issue, but having reasonable security is. For instance, the U.S. Department of Homeland Security recently ran a test in 2011 where staff secretly dropped USB drives and CDs in the parking lots of government buildings and private contractors.[56] Of those who picked up the media, an overwhelming 60% plugged them into office computers to see what they contained.[57] If the drive or CD had an official logo, 90% were installed.[58] "The test showed something computer security experts have long known: Humans are the weak link in the fight to secure networks against sophisticated hackers."[59]

Moving forward, legislation and international treaties should focus on the immediate concern regarding cyber security, not on hypothetical accounts of "war." Addressing security is practical--attacks are less likely to succeed on secured systems and networks with diligent operators, especially given that the majority of breaches today are as a result of system failures and employee negligence.[60]

A study from the Computer Security Institute (CSI) showed that 64.3% of companies surveyed experienced malware infections, 29.2% experienced denial-of-service attacks, 17.3% experienced password sniffing, and 16% experienced web defacement.[61] Upon further analysis based on an Accenture study on corporate data security, cyber crime was found to be the cause for only 18% of security breaches, while system failure accounted for 57% and employee negligence accounted for 48% of data loss.[62] Many careless individuals are uninformed about techniques used to compromise information, such as phishing.[63] Although organizations have written guidelines on internal security protocols, they fail to enforce them, and employees are often unaware of policies that, for instance, prohibit them from taking laptops home or from inserting media drives into their work computers.[64] Perhaps the most effective defense against "cyber war" is increased due diligence, better IT training, and improved security measures, especially given that approximately 85% of critical network infrastructure is privately owned.[65]

According to Howard Lipton from the CERT[66] Coordination Center, "[p]erhaps the greatest threat to the Internet today is the abysmal state of security of so many of the systems connected to it."[67] One problem lies with commercial off-the-shelf software where the number of features and time to market outweigh the security design, and new vulnerabilities are continuously found in most new software.[68] Widespread use means that one exploit could be targeted at millions of systems that have the vulnerable product installed, and a lack of security expertise by most Internet users means that vendor security patches will not be timely installed.[69] As a result, these systems are easily compromised by attackers, who may then use the systems to launch additional attacks against better-protected systems, and to hide the source(s) of the attack.[70]

56 *See* Michael Riley, *Human Errors Fuel Hacking as Test Shows Nothing Stops Idiocy,* Bloomberg, Jun. 27, 2011, *available at* http://www.bloomberg.com/news/2011-06-27/human-errors-fuel-hacking-as-test-shows-nothing-prevents-idiocy.html.

57 *See Id.*

58 *See Id.*

59 *Id.*

60 *See infra* Part IV(B).

61 14th Annual CSI Computer Crime and Security Survey, December 2009, *available at* pathmaker.biz/whitepapers/CSISurvey2009.pdf.

62 Creating a culture of caring regarding data privacy and protection, Accenture (Apr. 27, 2010), https://microsite.accenture.com/dataprivacyreport/Pages/default.aspx.

63 Phishing is the act of sending an e-mail to a user falsely claiming to be an established enterprise in an attempt to scam the user into surrendering private information, such as a login and password. *See* What is Phishing? – A Word Definition from the Webopedia Computer Dictionary, http://www.webopedia.com/TERM/P/phishing.html (last visited Jan. 4, 2011).

64 *See Id.*

65 Critical Issues for Cyber Assurance Policy Reform, Intelligence and National Security Alliance (Mar, 2009), http://www.insaonline.org/assets/files/INSA_CyberAssurance_Assessment.pdf

66 The United States Computer Emergency Readiness Team (US-CERT) is charged with providing response support and defense against cyber attacks for the Federal Civil Executive Branch (.gov) and information sharing and collaboration with state and local government, industry and international partners. *See* US-CERT: About Us, *http://www.us-cert.gov/aboutus.html* (last visited Jan. 5, 2010).

67 Howard F. Lipson, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues,* Nov. 2002, CERT Coordination Center [hereinafter Lipton] at 9.

68 *See Id.*

69 *Id.*

70 *Id.*

The expertise of the average systems administrator has also continued to decline.[71] In the early days, a relatively small number of systems were attached to the network, which were administered by individuals possessing the skill required to configure and maintain basic system security.[72] Today, the growing numbers of systems attached to the Internet are operated by users with little or no security or administrative expertise, such as the majority of ordinary consumers who own a PC or Mac.[73] These machines become easy prey for attackers. Furthermore, the Internet today has become decentralized, channeling across international boundaries and countless administrative domains, and there is no uniform monitoring system, or a central administrative control.[74] In the absence of cooperation, there is no global visibility, because no entity can monitor or trace outside of its own administrative domain.[75]

IV. Legal Responses

Cyber security legislation is a double-edged sword, on one side it purports to mitigate lost revenue due to cyber attacks; on the other it will increase transactional costs associated with online businesses, which may bar smaller entities from market entry. In 2010, the Internet economy accounted for 4.7% of the United States GDP, and 5% of all retail sales.[76] The Internet contributed more as a percentage of America's GDP than traditional industries such as information and technical services, construction, education, agriculture, entertainment, and recreation.[77] A growing number of Americans today are making a living online, from small website owners and blog writers who monetize content through ads and affiliate links, to small retailers who utilize a virtual store front to ship goods directly from the warehouse to the consumer. Moving forward, legislators must tread carefully, as any resultant government intrusion will undoubtedly incur a cost.

Of chief concern to both public and private sectors is the need for *reasonable* security, in the form of (1) improved standards for hardware and software systems, and network protocols; (2) improved training and due diligence of operators and employees; and (3) accountability for those responsible for data or security breaches. Secondary, there is also a need for improved coordination, visibility, and shared control of network infrastructure internationally in order to track, respond to, and isolate attacks.

Cyber security has been of concern since the late 90's, and several industry-specific laws have already been passed over the years. The Gramm-Leach-Bliley Act ("GLB") of 1999 requires financial institutions to implement comprehensive safeguards to protect customer information from foreseeable threats in security and data integrity.[78] The Federal Information Security Management Act ("FISMA") of 2002 implemented minimum security requirements for each federal agency and certification requirements for its contractors.[79] Internationally, the U.S. signed onto the Council of Europe's Convention on Cybercrime, a common criminal policy aimed at protection of society against cybercrime.[80] Specifically it enumerates clear substantive offenses, such as copyright infringement, computer-related fraud, breaches of network security, and child pornography. [81] Both GLB and FISMA were narrowly tailored, risk-based policies for cost-effective security, and the Convention merely reiterates domestic criminal law on an international stage. However, recently proposed bills--security concerns polluted with the rhetoric of cyber war--seem to have far-reaching effects.

Most controversial was perhaps S. 773, the Cybersecurity Act of 2010,[82] which purported to give the President authority to "shutdown Internet traffic to and from any compromised federal government or United States critical infrastructure[83] information system or network."[84] "Critical infrastructure" includes sectors of "agriculture, food, water, public health, emergency services ,government, defense

71 Lipton at 16.

72 *Id.*

73 *See Id.*

74 *Id* at 16-17.

75 *Id.*

76 Courteney Palis, *Internet Economy: How Essential Is The Internet To The U.S.?* Huffington Post, Mar. 20, 2012, *available at* http://www.huffingtonpost.com/2012/03/20/internet-economy-infographic_n_1363592.html.

77 *See Id.*

78 Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999, *available at* http://www.gpo.gov/fdsys/pkg/PLAW-106publ102/content-detail.html.

79 *See* 44 U.S.C. § 3541, et seq.

80 Convention on Cybercrime, Nov. 23, 2001, E.T.S. No. 185, *available at* http://www.conventions.coe.int/Treaty/en/Treaties/Html/185.htm.

81 *See Id.*

82 S. 773, 111th Cong. (2009), *available at* http://www.opencongress.org/bill/111-s773/text.

83 Being designated as a critical infrastructure also incurs obligations for upgrades and compliance. *See Id.*

84 *Id.*

industrial base, information and telecommunications, energy, transportation ,banking finance ,chemicals and hazardous materials, and postal and shipping," an exhaustive list spanning across both public and private institutions.[85] Such language is extremely broad, and gives the executive discretion to flip what critics have dubbed an "Internet kill switch."[86] Under heavy scrutiny, the bill ultimately died, but it brought to light existing emergency powers conveyed to the president from Section 706 of the Communications Act of 1934, which it purported to limit--an "Internet kill switch" already exist.

Section 706 expressly provides that "[u]pon a proclamation by the President that there exists war or threat of war, or a state of public peril or disaster or other national emergency," the President, "in the interest of national security or defense . . . may cause the closing [or use] of any station . . . or device . . . upon just compensation to the owners."[87] The President may also amend or suspend the rules and regulations applicable to "any or all facilities or stations within the jurisdiction of the United States."[88] This power applies to both "radio communication" and "wire communication,"[89] defined as "transmission of writings, signs, signals, pictures, and sounds of all kinds," as well as all things "incidental to such transmission."[90] Although it is difficult to argue that Congress had the Internet in mind when they passed the legislation over 70 years ago, the language seems to encompass all Internet infrastructure. Herein lies the danger of confusing issues of cyber security with war, "war" authorizes the President to take property.

What would a "shutdown of the Internet" mean? Is it even possible? Although the "kill switch" rhetoric might be overblown, the damage would still be severe. Simply stated, the Internet cannot be shut down because of its decentralized characteristics.[91] The President would however, be able to take segments of the network off the Internet. What would likely happen, in the event of an attack of sufficient degree, is that an administrative official will instruct an operator to block certain incoming packets from certain source addresses, or perhaps temporarily, to block all incoming addresses. Fortunately, two limitations on the 1934 Act exist to protect consumers and businesses: (1) the power can only be exercised in an emergency; and (2) just compensation would be required for any downtime. The Cybersecurity Act of 2010 had no such restrictions.

Recently, the Cybersecurity Act of 2012 has been reintroduced, without the kill switch provision.[92] However, this bill introduces new privacy concerns, for instance it allows any *private* entity to "monitor information systems," "operate countermeasures," and to "disclose any "cybersecurity threat indicators" to any other private entity.[93] "Cybersecurity threat" is defined as "any action that *may* result in unauthorized access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, or availability of an information system or information that is stored on, processed by, or transiting an information system" (emphasis added).[94] The language of course, is intentionally vague, and basically allows any one of CYBERCOM's private contractors to freely monitor and share any online activity of any online actor.

Unfortunately, the "cyber war" rhetoric has found its way into an umbrella of other related bills. For instance, the National Defense Authorization Act[95] declared the Internet as an "operational domain" in the war on terror, and includes authorization to indefinitely detain citizens on suspicion of supporting or sympathizing with broadly defined terrorists, as well as anyone who commits a "belligerent act."[96] Also as part of the bill, the U.S. military now has authorization to conduct "offensive" strikes online, despite there being zero documented hacking attacks on U.S. infrastructure—a recent report that a water pump in Illinois had been destroyed by Russian hackers turned out to be a contractor logging in from his vacation, at the request of the water company.[97]

85 *Id*.

86 State of the Union With Candy Crowley, CNN.com, http://transcripts.cnn.com/TRANSCRIPTS/1006/20/sotu.01.html

87 Communications Act of 1934, Section 706, *available at* http://www.fcc.gov/Reports/1934new.pdf.

88 *Id*.

89 *See Id*.

90 *See* Comm. Act 1934 Sec. 3

91 *See infra* Part III(A).

92 S. 2105, 112th Cong. (2011-2012), *available at* http://www.govtrack.us/congress/bills/112/s2105.

93 *Id* at 153.

94 *Id* at 182.

95 H.R. 1540, 112th Cong. (2011), signed into law Dec. 31, 2012, *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr1540enr/pdf/BILLS-112hr1540enr.pdf.

96 *See Id* at Sec. 1031(b)(2).

97 Ryan Singel, *Congress Authorizes Pentagon to Wage Internet War*, Wired, Dec. 14,

Conclusion

What is "cyber war?" Does it even exist? The short answer is no, at least not until we start it. The recent hypothetical accounts of cyber warfare have captured attention of the media and harnessed the imagination of Americans. People scare easily, and there is a profit to be made from scaring people. "Cyber war" has been used as a catch-all phrase, commonly confused with cyber crime, cyber espionage, and hacktivism.[98]

"Cyber war" is not an issue of war, and the laws covering kinetic warfare is an ill fit. All-out cyber warfare between nations is science fiction, in a world where we all share the same underlying domain, and are all dependent on the same global economy. Instead of authorizing armed attacks in response to imagined cyber threats as a deterrent, attention should be focused on prevention through reasonable cyber security.

Today, the majority of critical network structure is privately owned, and in reality, disruptions, loss in data, and security breaches are mostly the result of human error, hardware failures, abysmal network and system security, and the lack of network visibility.[99] Preventive security does not require a "re-engineering" of the Internet, and care must be taken to preserve its openness, which created an expanding culture for innovation in the arts, sciences, and technology. Moving forward, legislators must tread carefully, because any resultant government intrusion will undoubtedly incur a price. Legislators will have to weigh the incremental benefits in security against the cost incurred on the private sector, as well as refine the legislative language, since its broad brush will affect everyone and everything on the Internet.

2011, *available at* http://www.wired.com/threatlevel/2011/12/internet-war-2.

98 *See supra* Part I(B).

99 *See supra* Part IV(B).

About the Author

Tony S. Guo is an IT and legal consultant with over 10 years of web development experience. He holds a B.S. in Computer Engineering from Purdue University, and a J.D. from the University of Miami School of Law.

Through his career, Tony has used web technologies to enhance legal advocacy, from writing databases for legal services, to designing websites for community organizations. He has spoken on cyberwar and international law at the University of Leipzig, and on legal outreach and the web at Harvard University.

Tony is a strong advocate for network neutrality, and believes in a maintaining an open and unbiased domain.

Air Force Research Laboratory's In-Residence Professor Becomes Cybersecurity Preceptor in South Korea

By Kevin Kwiat

The Air Force Research Laboratory (AFRL) is fortunate to have one of its subject matter experts (SMEs) working hand-in-hand with South Korea as it looks to advance its cybersecurity capabilities. This SME acquired his expertise prior to his affiliation with AFRL. In recognition of his knowledge, South Korea's cybersecurity endeavors spurred an invitation to Syracuse University Professor Dr. Joon Park. Dr. Park now supports the AFRL's Information Directorate (AFRL/RI) in Rome, NY, under the auspices of the Air Force Office of Scientific Research (AFOSR) funded National Research Council (NRC) Research Associateship Programs (RAP). Through RAP, he is a senior research fellow on a multi-year extended sabbatical. Over the past decades, Dr. Park has been involved with theoretical and practical research and education in information and systems security. He has been integral in establishing Syracuse University as a National Security Agency and Department of Homeland Security-designated Center of Academic Excellence in Information Assurance (IA) both for education and research. He is also the principal investigator for the Department of Defense Information Assurance Scholarship Program at Syracuse University.

Although Dr. Park's RAP activities primarily aim to contribute to the Directorate's cyber assurance research and facilitate collaboration with Syracuse University, the broad and in-depth impact in cybersecurity that he achieved as a university professor had already positioned him as a forerunner in the field. During his first year of RAP tenure, Dr. Park's work at Syracuse University allowed him to create a series of seminars and tutorials for South Korea's world-class universities and multi-national flagship information technology (IT) companies, such as Korea Advanced Institute of Science and Technology, Yonsei University, Korea Institute of Science and Technology, and Samsung Electronics.

Embracing advanced technology and emphasizing high vigilance are two mindsets that go together in South Korea. With 95% of its households having a permanent Internet connection, the country is leading the world in what it means to be "wired." This strong measure of progress is blended with apprehension because of South Korea's locale; it is a region of unsurpassed armament. Similarly, cyberspace exhibits the properties of progress and, with the ever-presence of threats, the potential for peril. Unlike kinetic weapons that invoke the fear of immediate physical harm, attacks within cyberspace have an invisible quality; therefore, defending against them is more diffuse. Being a high-profile occupant of cyberspace has meant that South Korea's interests in securing its Internet presence have spanned its government, military, industrial, and civilian sectors. Recently, Dr. Park has played a key role in its efforts.

He leads research seminars in South Korea, which are intended for IA researchers, security administrators, and IT system developers, that explore how to apply information security technologies and approaches to real-life systems and services. Based on the demand by the current technology trends and evolution, Dr. Park presents the evolution of security challenges, potential solutions, and related issues in popular IT services, including cloud computing, online social networking, biometrics, and mission-critical systems.

His IA tutorials cover the principal concepts and approaches in information security for executive decision makers within organizations and general IT practitioners. His comprehensive approach considers not only technical solutions, but also non-technical issues related to information security management, including principal concepts of information security, system vulnerabilities, information security policies, models, mechanisms, and evaluation.

The outcome of Dr. Park's South Korean endeavors exceeded expectations. The goal for his trips was education and dissemination, but he achieved much more. He generated enthusiasm, and enthusiasm can be infectious. As a professor whose primary research and teaching area is information security, he has been trying to share his research outcomes and teaching philosophy so that, ultimately, the cybersecurity knowledge and practice can make a positive impact on the entire society. Dr. Park's presentations in South Korea were based on work he accomplished prior to his RAP tenure at AFRL, but the spreading of cybersecurity understanding to

South Korea has been aligned with AFRL's interests. Dr. Park's activities follow closely upon AFRL's recent investment in South Korea's Pohang University of Science and Technology. The university completed a research grant through AFOSR's Asian Office of Aerospace Research and Development.

The Pohang University effort entitled "Distributed Detection of Attacks/Intrusions and Prevention of Resource-Starvation Attacks in Mobile Ad Hoc Networks" is aimed squarely at improving mission-based cyber defense; it sought to assure mission-essential functions by preserving scarce battery power during attack avoidance in wireless settings. The research has synergies with AFRL's similar endeavors to adapt concepts from the domain of fault-tolerant computing to achieve information assurance in an in-house, AFOSR-funded effort called "Fault Tolerance for Fight Through (FTFT)." In particular, an AFRL-developed protocol to tolerate attacker-caused faults in mobile wireless units while preserving the units' battery power underscored the complementary nature of threat avoidance and surviving the threat, which was exhibited by the respective Korean and AFRL research.

Dr. Park has provided exemplary support to the FTFT effort through his innovation in creating novel approaches for component survivability at runtime in mission-critical distributed systems. His approaches embrace the early adoption of emerging—yet unproven—technology; the rapid recovery of component failure; and the use of commercial-off-the shelf components. Dr. Park's compelling demonstrations of his ideas bring AFRL closer to creating cyberspace foundations that are trusted, resilient, and affordable. Leveraging from the research gains achieved in discovering fight-through schemes, he is addressing trust and privacy issues in online social networks. Today, the adoption of online social media and their applications have expanded in kind and size to unprecedented levels and continue to grow at accelerated rates. The creation and deployment of social media is one of the main forces behind the evolution and expansion of the Internet and mobile media. Social media accounts for the majority of Internet traffic while its content comprises the greater part of the daily published multi-media on the Internet. These technologies have a profound impact on society; yet, they can have detrimental outcomes if used maliciously. Inadvertent usage of online social networks may compromise the user's privacy.

Additionally, researchers note that an oppressive regime, for example, could misuse its users' social network to cause a dramatic loss in society's trust of technology. Such a regime could then assert more political control because the loss of trust would undermine the network's ability to form linkages

Figure 1 Dr. Park lecturing at Samsung in South Korea

among people. Dr. Park's investigations in the building and maintaining of trust in social networks holds promise for finding a guiding science to better understand the evolution of this technology—a technology that is a microcosm of the Internet and mobile media.

Defense of cyberspace is challenging. The seemingly endless breadth of cyberspace coupled with the technological depth of its composition can divide defensive approaches to be either overarching or highly specific. To abstract away details for the purpose of tractability, overarching approaches can suffer because simplistic models for threats, vulnerabilities, and exploits tend to yield defenses that are too optimistic. Approaches that deal with specific threats, vulnerabilities, and exploits may be more credible, but can quickly lose their meaningfulness as technology changes. Whether approaches are near- or far- term, FTFT's maintains two goals: the ability to survive and the ability to fight-through. Maintaining such a stance requires a healthy dose of skepticism of a technology's ability to be defensible.

Dr. Park's tangible recent research contributions to AFRL/RI have been through FTFT; yet, if enthusiasm is indeed infectious, then the FTFT effort, and therefore AFRL/RI, is also a beneficiary of his South Korean experiences.

A primary part of any research is a proper perspective. Dr. Park's infusion of the in-house research, his renewed perspective that embraces advanced technology, and his emphasis on high vigilance is a sound prospect for the future of cybersecurity in South Korea and abroad.

About the Author

Dr. Kevin A. Kwiat is a Principal Computer Engineer in the Cyber Assurance Branch of the AFRL in Rome, NY where he has worked for over 28 years. He received his B.S. in Computer Science, B.A. in Mathematics from Utica College of Syracuse University, as well as his M.S. in Computer Engineering and the Ph.D. in Computer Engineering from Syracuse University. He is an NRC Adviser, acting as a surrogate of the NRC in monitoring his designated research associates and all matters relating to an associate's research program fall under his purview.

"Approved for Public Release; Distribution Unlimited: 88ABW-2012-2539, 30-APR-2012"

First Consolidated Basic Center Operations Contract to Quanterion

By Preston MacDiarmid, President Quanterion Solutions Incorporated

Quanterion Solutions is thrilled to be competitively selected to operate the Department of Defense (DoD) Cyber Security and Information Systems (CSIAC) Basic Center Operations (BCO), the first consolidated Information Analysis Center (IAC) contract. The consolidation includes three previous IACs: the Information Assurance Technology Analysis Center (IATAC) previously operated by Booz, Allen and Hamilton, the Modeling & Simulation Information Analysis Center (MSIAC) operated by Alion Science and Technology and the Data and Analysis Center for Software (DACS) operated by Quanterion Solutions. The CSIAC also includes a new technology area, Knowledge Management/Information Sharing.

Quanterion Solutions Incorporated was formed in 2000 as a small business to perform services for government and industry using QUANTitative critERION for decision-making, hence the name Quanterion. The company of four has grown to more than forty in twelve years, rapidly expanding its technical services and customer base. While its beginning focused on services in reliability, maintainability and quality, it has since grown to address materials engineering, software engineering/development and information assurance/cyber security. Its software products include desktop engineering analysis tools as well as asynchronous on-line training courses.

The company skills in operating IACs come from a long line of current and past IAC Directors, Deputy Directors and other key personnel with more than 110 cumulative years helping to make the program a success. Past Directors Dave Rose (Advanced Materials, Manufacturing and Testing IAC (AMMTIAC)), Tom McGibbon (DACS) as well as RAC/RIAC's Dave Nicholls and Dave Mahar are well known in IAC-circles.

After leaving the IAC business area to form Quanterion, 2005 represented the re-entry of the company staff into the IAC program when a Quanterion assembled team with Wyle Laboratories as the prime was awarded a competitive contract to operate the Reliability Information Analysis Center (RIAC), with the "I" for "information" added to "RAC" to emphasize that the Center is part of the IAC program. In 2010 IAC Program's contracting strategy was restructured to introduce greater competition for customer-funded tasks and to create more opportunities for small business in the program. As a result, Quanterion was successful in competing as a small business to operate the DACS Basic Center Operations (DACS BCO).

While the company's staff has been successful in operating IACs for a long time, the information world has undergone tremendous change. It's obvious that the IAC operating teams

The CSIAC award marks the start of a new phase in the highly successful DoD IAC program, reducing the ten previous IACs to three, while at the same time expanding the breadth of the Center's technical scope. Next on the horizon is the expected January of 2013 award of the Homeland Defense and Security IAC (HDIAC), expanding the current Chemical, Biological, Radiological and Nuclear IAC (CRRNIAC) currently operated by Battelle to add Biometrics, Medical, Cultural Studies and Alternative Energy. The third Center is planned for award in September of 2013 consolidating the Reliability Information Analysis Center (RIAC), the Advanced Materials, Manufacturing and Testing IAC (AMMTIAC), the Weapon Systems Technology IAC (WSTIAC), the Sensors IAC (SENSIAC), the Chemical Propulsion IAC (CPIAC) and the Survivability/Vulnerability IAC (SURVIAC).

have to continuously change accordingly, continuing to make the right data and information available, in the most effective formats, in a timely manner. We also have the challenge to capture the lessons-learned knowledge of our rapidly aging technical workforce, now in a truly global economy. A recent independent study performed by the Center for Strategic and International Studies (CSIS) acknowledges the IACs' contributions, specifically in the areas of "data-to-decisions", "better buying power" and "acquisition support."

We believe that we have effective and innovative plans for our IAC work in the future, but we certainly don't have all the answers. We welcome your ideas as IAC customers regarding how we can serve you better. What do you need to do your job better? Think in terms of data/information, tools/models, publications/ critical technology assessments, and/or training? We have the flexibility in our IAC contracts to be responsive to your needs, so please let us know what they are by contacting:

- Software Engineering & Knowledge Management/ Information Sharing Needs: Tom McGibbon, tmcgibbon@quanterion.com
- Cyber Security/Information Assurance Needs: Michael Weir, mweir@quanterion.com
- Modeling & Simulation Needs: Steve Swenson, sswenson@aegistg.com
- Reliability, Maintainability, Quality Needs: Dave Nicholls, dnicholls@quanterion.com.

About the Author

Mr. MacDiarmid is the President of Quanterion Solutions Incorporated, a twelve-year old engineering and software development company (quanterion.com) emphasizing knowledge management and information center operation. Previous to forming Quanterion, Mr. MacDiarmid was Director of the Reliability Analysis Center (now RIAC) for ten years and Vice President of Information Analysis Center (IAC) Operations for IIT Research Institute (IITRI) (now Alion). Mr. MacDiarmid holds a BSME from the University of Buffalo, an MSME from Syracuse University, and an MBA from Rensselaer Polytechnic Institute. He is an ASQ Certified Reliability Engineer, a Senior Member of the IEEE Reliability Society, and a Member of the ASME. He was the Mohawk Valley Engineers Executive Council 2002 Excellence in Engineering Award Winner for his contributions to the field of reliability. Under his leadership, Quanterion Solutions was presented the 2007 Mohawk Valley "Leading Edge" award for the company's technical work.

RECENT IAC PROGRAM RESTRUCTURING

BEFORE 2010:

Traditional IAC contracts include two parts: "core operations" and major customer funded Indefinite Delivery/Indefinite Quantity (IDIQ) tasks.

2010:

- IAC Program restructured to have separate "Basic Center Operations (BCO) contract for each of ten IACs and three sets of Multiple Award Contracts (MACs) for consolidations of the ten IAC technologies major customer-funded tasks.
- Nine MAC contracts were awarded to be able to further compete the major customer-funded tasks previously covered by the IATAC, the MSIAC and the DACS. The new contracts were named SNIM for Software, Networks, Information, and Modeling and Simulation.
- The first new IAC BCO (DACS) was awarded to Quanterion Solutions.

2011:

The Government's restructuring plans were changed to consolidate the BCOs along the same technology lines as the MACs reducing the planned ten BCOs to three.

2012:

The first consolidated BCO, the CSIAC was awarded to Quanterion Solutions.

2013:

The Government plans to award BCO contracts for the Homeland Defense and Security IAC (HDIAC) and the Defense Systems IAC (DSIAC) as well as sets of MAC contracts for both the Homeland Defense Technical Area Task (HD TATs) and the Defense Systems Technical Area Tasks (DS TATs).

The CSIAC Technology Areas Support Team

GEORGE MASON UNIVERSITY

GEORGE MASON UNIVERSITY | Center for Infrastructure Protection and Homeland Security

Established in 2002, CIP/HS is based at George Mason University School of Law in Arlington, Virginia. The Center integrates law, policy, and technology to conduct comprehensive analyses and research, including strategic planning, resiliency studies, independent program assessments, security evaluations, educational initiatives, conferences, white papers, and recommendations relevant to improving the safety and security of the United States and its allies. Today, the Center for Infrastructure Protection and Homeland Security features NIST-funded core research projects as well as sponsored research projects. Through an extensive network of subject-matter experts and partnerships with industry; academia; and federal, state, and local officials, our team of dedicated professionals is uniquely positioned to address concerns across all eighteen CIKR sectors. CIP/HS' approach to cybersecurity is multi-disciplinary and international, integrating research and education in law, policy, and technology. The Center seeks practical, implementable solutions to operational needs to secure critical transnational cyber networks.

AEGIS TECHNOLOGIES

AEgis TECHNOLOGIES

Founded in 1989, AEgis Technologies brings to CSIAC twenty-three years experience in modeling and simulation, software design and development, simulator design, development, and deployment, information assurance, and software and systems engineering. A privately held small business headquartered in Huntsville, Alabama, AEgis provides advanced technology and expert consulting services to industries throughout the world, specializing in modeling & simulation (M&S), software engineering, information assurance, micro/nanoscale technology development, and systems engineering. The company's M&S products and services include simulation software and training simulators; geospatial databases; 3D models; war fighter exercise support; systems engineering and analysis; verification, validation, and accreditation (VV&A); test and evaluation support, and both Hardware-in-the-Loop (HWIL) and Man-in-the-Loop (MIL) simulation. AEgis additionally provides commercial modeling and simulation software tools, motion-based maneuver trainers, MEMS, Photonics, and microfluidic devices to industries around the world.

SRC, INC

SRC Defense › Environment › Intelligence
Redefining possible®

SRC, Inc. is a not-for-profit Department of Defense-focused research and development company with over 50 years experience in defense, environment and intelligence applications. SRCTec, Inc., a wholly owned subsidiary of SRC, provides manufacturing and logistics support for complex electronics systems. With corporate headquarters located in North Syracuse, NY, SRC and SRCTec employ over 1,100 people in 14 offices and numerous support locations throughout the U.S. SRC provides information assurance (IA) and information operations (IO) products and services to various agencies across the intelligence community, as well as in the homeland security domain. This includes IA operations support, IA policies and programs, IA protection engineering and IA risk analysis. SRC designed, developed and operates a security operation center that enables the monitoring of information technology assets 24 hours a day, to evaluate and respond to cyber security threats.

AIS, INC

AIS Inc. is a Small Business headquartered in Rome NY, with offices in Catonsville MD, Portland OR, Dayton OH, and Omaha NE. The company performs research and development in computer network operations and security for U.S. Government customers. AIS, Inc. started as a pioneer in research and development in the domains of cyber adversarial sciences and computer network operations, and now specializes in the rapid development of unique cyber capabilities, as well as the associated infrastructure that enables effective and controlled use of computer network operations tools to achieve national objectives across the entirety of the cyber domain.

SYRACUSE UNIVERSITY

School of Information Studies
SYRACUSE UNIVERSITY

Syracuse University teams the iSchool and the CASE Center to build and support the CSIAC. The SU School of Information Studies at (iSchool) was the first "information school" in the nation. It is a leading center for innovative programs in knowledge, information systems, information technology, and information services. The iSchool brings a great deal of experience in the transformation of digital libraries into communities of practice. That work includes extensive expertise in information retrieval, open source software, metadata development, and the architecture of collaboration. This work includes the development of community systems for the U.S. Department of Education including extensive semantic web technologies for the efficient gathering, organizing and re-distribution of educational materials. Syracuse University's CASE (Center for Advanced Systems and Engineering) is New York State's premier applied research center for interdisciplinary expertise in complex information intensive systems, including monitoring and control, predictive analysis, intelligence, security and assurance. CASE offers expertise in data fusion, data mining, systems modeling and analysis, bioinformatics, systems security and assurance, intelligent computing, and sensor networks. The DACS will leverage their leading position among universities and state-of-the- art research in web-based information collection and collaboration technology.

UNIVERSITY OF SOUTHERN CALIFORNIA (USC)

USC CSSE Center for Systems and Software Engineering

The University of Southern California (USC) Center for Systems and Software Engineering, founded by Dr. Barry Boehm in 1993, is part of USC's Viterbi School of Engineering. This Center is well-known for its research and development of practical software technologies that can aid industry in reducing cost, customizing designs, and improving design quality. Current focus areas of research within the center include the incremental commitment spiral model which is a refinement of the original spiral model, COCOMO cost-schedule-quality estimation model extensions, systems engineering cost estimation, and agile methods. As part of mutual on-going collaborations, CSIAC and USC developed the Software and Systems Cost and Performance Analysis Toolkit (S2CPAT) that contains software engineering cost and schedule information for over 300 major defense acquisition programs that can be used to support software cost estimation and software engineering research.

Article Submission Policy

The CSIAC Journal is a quarterly journal focusing on scientific and technical research & development, methods and processes, policies and standards, security, reliability, quality, and lessons learned case histories. CSIAC accepts articles submitted by the professional community for consideration. CSIAC will review articles and assist candidate authors in creating the final draft if the article is selected for publication. However, we cannot guarantee publication within a fixed time frame.

Note that CSIAC does not pay for articles published.

AUTHOR BIOS AND CONTACT INFORMATION

When you submit your article to CSIAC, you also need to submit a brief bio, which is printed at the end of your article. Additionally, CSIAC requests that you provide contact information (email and/or phone and/or web address), which is also published with your article so that readers may follow up with you. You also need to send CSIAC your preferred mailing address for receipt of the Journal in printed format. All authors receive 5 complementary copies of the Journal issue in which their article appears and are automatically registered to receive future issues of Journal. Up to 20 additional copies may be requested by the author at no cost.

COPYRIGHT:

Submittal of an original and previously unpublished article constitutes a transfer of ownership for First Publication Rights for a period of ninety days following publication. After this ninety day period full copyright ownership returns to the author. CSIAC always grants permission to reprint or distribute the article once published, as long as attribution is provided for CSIAC as the publisher and the Journal issue in which the article appeared is cited. The primary reason for CSIAC holding the copyright is to insure that the same article is not published simultaneously in other trade journals. The Journal enjoys a reputation of outstanding quality and value. We distribute the Journal to more than 30,000 registered CSIAC patrons free of charge and we publish it on our website where thousands of viewers read the articles each week.

FOR INVITED AUTHORS:

CSIAC typically allocates the author one month to prepare an initial draft. Then, upon receipt of an initial draft, CSIAC reviews the article and works with the author to create a final draft; we allow 2 to 3 weeks for this process. CSIAC expects to have a final draft of the article ready for publication no later than 2 months after the author accepts our initial invitation.

For some issues CSIAC has a Guest Editor (because of their expertise) who conducts most of the communication with other authors. If you have been invited by a Guest Editor, you should submit your article to them per the email address they provide and follow their instructions. Otherwise, articles should be emailed to John Dingman, Managing Editor for the Journal. See contact information below.

PREFERRED FORMATS:

- Articles must be submitted electronically.
- MS-Word, or Open Office equivalent (something that can be edited by CSIAC)

SIZE GUIDELINES:

- Minimum of 1,500 – 2,000 words (3-4 typed pages using Times New Roman 12 pt font) Maximum of 12 pages
- Authors have latitude to adjust the size as necessary to communicate their message

IMAGES:

- Graphics and Images are encouraged.
- Print quality, 200 or better DPI. JPG or PNG format preferred

Note: Please embed the graphic images into your article to clarify where they should go but send the graphics as separate files when you submit the final draft of the article. This makes it easier should the graphics need to be changed or resized.

CONTACT INFORMATION:

CSIAC
100 Seymour Road Suite C102
Utica, NY 13502
Phone: (800) 214-7921
Fax: 315-351-4209

John Dingman, Managing Editor
Phone: (315) 351-4222
Email: jdingman@quanterion.com

Tom McGibbon, CSIAC Director
Phone: (315) 351-4203
Email: tmcgibbon@quanterion.com

CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC), technically managed by the Air Force Research Laboratory (AFRL) in Rome, NY and operated by Quanterion Solutions Incorporated, Utica, NY.

ABOUT THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

ARTICLE REPRODUCTION

Images and information presented in these articles may be reproduced as long as the following message is noted:

"This article was originally published in the Journal of Cyber Security and Information Systems Vol. 1, No. 1 October 2012."

In addition to this print message, we ask that you notify CSIAC regarding any document that references any article appearing in the *CSIAC Journal.*

Requests for copies of the referenced journal may be submitted to the following address:

Cyber Security and Information Systems
100 Seymour Road
Utica, NY 13502-1348

Phone: 800-214-7921
Fax: 315-351-4209
E-mail: info@thecsiac.com

An archive of past newsletters is available at **https://journal.thecsiac.com.**

Distribution Statement:
Unclassified and Unlimited

CSIAC
100 Seymour Road
Utica, NY 13502-1348
Phone: 800-214-7921
Fax: 315-351-4209
E-mail: info@thecsiac.com
URL: http://www.thecsiac.com/

ABOUT THIS PUBLICATION

The Journal of Cyber Security and Information Systems is published quarterly by the Cyber Security and Information Systems Information Analysis Center (CSIAC). The CSIAC is a DoD sponsored Information Analysis Center (IAC), administratively managed by the Defense Technical Information Center (DTIC). The CSIAC is technically managed by Air Force Research Laboratory in Rome, NY and operated by Quanterion Solutions Incorporated in Utica, NY.

Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the CSIAC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the CSIAC, and shall not be used for advertising or product endorsement purposes.

ABOUT THE COVER

Cover Design

Shelley Howard (Quanterion Solutions, CSIAC)

Photo Credit

U.S. Air Force 1st Lt. Jamie Leenman, a pilot assigned to the 21st Airlift Squadron, operates mission index flying software on an Air Mobility Command mission laptop computer aboard a C-17 Globemaster III aircraft at Travis Air Force Base, Calif., Feb. 15, 2012. To use the software, Airmen enter various aircraft and atmospheric parameters on a laptop at different intervals during a mission, with the software providing them with speed and altitude recommendations for maximum aircraft performance and efficiency. **(U.S. Air Force photo by Ken Wright)**

Mission Index Flying is the military version of a civilian capability known as Cost Index Flying, or CIF. CIF balances the cost of time versus the cost of fuel, not just minimizing fuel use, but reducing operational costs across the enterprise, branching out into areas such as time-based maintenance and other enterprise costs.

Striving for fuel efficiency affects everyone in the command from air crews to the maintainers and support crew on the flightline.

AMC Fuel Efficiency Office's Mr. Eric Lepchenske said, "More than $842 million dollars has been taken out of the fuel budget from fiscal 2012 to 2017. Since fuel is a 'must-pay bill,' we are faced with a choice; we can implement efficiencies that gain $842 million or face possible cuts in other operational areas, such as flight hours if we are unable to do so. Implementing MIF is one attempt to avoid such cuts.

"If we are flying fewer hours because we can't meet that $842 million budget reduction, then there is a risk that there will be less need for the support and maintenance crews on the ground," said Lepchenske.

"We chose to the use the term Mission Index Flying because it is applies more readily to the military," said Mr. Lepchenske. "Although similar, the way AMC will utilize Mission Index Flying and handle the costs to our mobility enterprise is different when compared to how civilian aviation uses CIF."

Even though MIF is an air crew-centric system, everyone who works with aircraft or aviation fuel has a role to play in the fuel efficiency mission.

Cyber Security and Information Systems Information Analysis Center
100 Seymour Road
Suite C-102
Utica, NY 13502

Return Service Requested

Journal of Cyber Security and Information Systems – October 2012
Welcome to the New and Enhanced CSIAC

— IN THIS ISSUE —