VOLUME 4 NUMBER 2

JOURNAL OF CYBER SECURITY & INFORMATION SYSTEMS

Modeling and Simulation Data Integration – Inviting Complexity

Gary W. Allen, PhD
Deputy Director

Instrumentation Training Analysis
Computer Simulations and Support

US Army Europe - Joint Readiness
Multinational Center

ABSTRACT: *This paper is an overview of various issues that arise regarding complexity of data integration when multiple modeling and simulation architectures are used in a Live-Virtual-Constructive (LVC) simulation network. Points include such items as conversion of units, differing data formats, and effects on technology performance. Examples are given of ways to mitigate complexity and the paper concludes with recommendations for network designers.*

In the arena of modeling and simulation (M&S) data translation and integration is key to the success of every application. As the growth of sophistication in the ability to simultaneously apply live, virtual, and constructive simulation environments the ability to exchange data between environments and different architectures has grown in complexity.

The purpose of this paper is to serve as a primer to the challenges of data integration. The following discussion will present data characteristics, issues when employing different M&S architecture, and ways to mitigate the challenges of data interoperability. The paper will conclude with recommendations of tools and processes that will aid in the design of complex M&S environments.

While the focus of this article has to do with data the specific issue at hand is inviting complexity by introducing different data structures and architectures in an M&S network. Specifically, the simultaneous use of multiple M&S architectures introduces a level of complexity that will affect accuracy and performance. For the purpose of this discussion the Distributed Interactive Simulation (DIS) and the High Level Architecture (HLA) are used.

Data Integration

One of the fundamental challenges with data integration is establishing a common set of definitions. In this case the term 'data' is defined as:

> "Data is a general concept that refers to the fact that some existing information or knowledge is represented or coded in some form suitable for better usage or processing." (Retrieved May 31, 2015 Data Characteristics, Wikipedia)

That represented information or knowledge also has a set of characteristics that underscore the definition. These characteristics are generally describing data as being relevant, complete, accurate, and current (Linthicum, 2009, p. 1). At this point it is important to note that these

characteristics should be qualified as 'useful data'. The point being that it is possible to have an item that meets the given definition but minus these characteristics is of little value. The terms utility and value are indicative of another term that is frequently used when describing data – 'quality'. Some additional characteristics referring to the quality in addition to the four already listed are accessibility, consistency, and granularity (Characteristics, quizlet.com). The point of sharing these additional items is merely to show that data as a topic is of great importance which has garnered much investment of time for study. For the purposes of this paper, however, we will limit the list of characteristics to relevant, complete, accurate, and current.

As will be shown later, the crux of data integration revolves around format. Associated with format is the use of a variety of measures to represent a commonly named item or representation term. A representation term is a word, or a combination of words, that semantically represent the data type (value domain) of a data element (Representation, Wikipedia). For instance, consider the concepts of Speed and Location. These elements can become more complex when one considers that each can be represented by different units (Fig 1).

Figure 1 – Data Representations

In order to ensure an accurate exchange of information between these simulations a conversion must take place. That conversion begins the introduction of complexity in to the process and represents a progression that will continue to increase with the introduction of multiple simulation architectures and their associated data components (Fig 2). The graph is a simple representation of the concept and not meant to imply there is a one-to-one relationship between the two variables.

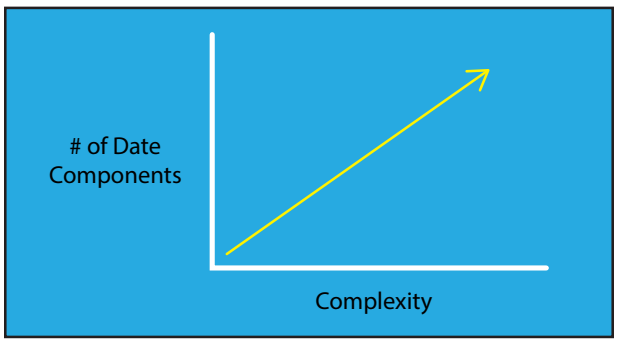


Figure 2 – Complexity Continuum

As previously mentioned accounting for differences in data format is a key requirement for system interoperability and a significant source of complexity. A simple example is a data element in one system is described using six bits and in another system that same element is described using eight bits. Some form of conversion must take place in order for these data bases to accurately exchange information. That conversion step is yet another source of complexity. The following example using DIS and HLA data elements shows how quickly the level of complexity can grow. Data elements in DIS are known as Protocol Data Units (PDUs). The current standard incorporates 72 different types of PDUs arranged in 13 families. Each PDU is comprised of 576 bits (IEEE, 2011, p. 67).

- Entity information/interaction family - Entity State, Collision, Collision-Elastic, Entity State Update, Attribute
- Warfare family - Fire, Detonation, Directed Energy Fire, Entity Damage Status
- Logistics family - Service Request, Resupply Offer, Resupply Received, Resupply Cancel, Repair Complete, Repair Response
- Simulation management family - Start/Resume, Stop/Freeze, Acknowledge
- Distributed emission regeneration family - Designator, Electromagnetic Emission, IFF/ATC/NAVAIDS, Underwater Acoustic, Supplemental Emission/Entity State (SEES)
- Radio communications family - Transmitter, Signal, Receiver, Intercom Signal, Intercom Control
- Entity management family
- Minefield family
- Synthetic environment family
- Simulation management with reliability family
- Live entity family
- Non-real time family
- Information Operations family - Information Operations Action, Information Operations Report

Given a single architecture network the issue of complexity is fairly easy to manage. When the network design begins to co-mingle simulation architectures the resultant incompatibility between data structures results in additional issues that in turn gives rise to tertiary effects. Let's look at the addition of HLA in order to better understand some of the issues involved.

The core data element for HLA is called a Basic Object Model (BOM). Like a DIS PDU the BOM structure captures a number of variables that describe an entity or Federate using HLA terminology (SISO BOM). Insight to the data integration problem is readily seen from comparing the components of an HLA BOM with that of the DIS PDU (Fig 3).

HLA Basic Object Model (BOM) Components	DIS PDU Components
› Model Identification	› Entity Information/Interaction
› Pattern of Interplay	› Warfare
› Pattern Action	› Logistics
› State Machine	› Simulation Management
› State	› Distributed Emission Regeneration
› Entity Type	› Radio Communications
› Event Type	› Entity Management
› HLA Object Class	› Minefield
› HLA Interaction Class	› Synthetic Environment
› HLA Attribute	› Simulation Management with Reliability
› HLA Parameter	› Information Operations
› Datatype	› Live Entity
› Enumerated Datatype	› Non-Real-Time Protocol
› Fixed Record Field	
› Variant Record Alternative	
› Basic Data Representation	
› Note	

Figure 3 – HLA DIS Comparison

The complex nature of exchanging data between DIS and HLA is further exacerbated in practice because each Federate is actually described by an expanded form of the BOM known as a Federation Object Model (FOM). The description of the fields that are part of a FOM requires 27 pages of text and is therefore far too long for use here (IEEE, 2010, p. 34). Certainly such extensive detail leads to greater fidelity in the simulation entities but this in turn also underlies the creation of tertiary effects which contribute further to the profile of network complexity. These items primarily have a negative effect on performance which must be addressed. The tertiary effects include such items as (Lessmann, E-mail):

- How much data is being distributed from each entity?
- What is the update rate for this data for each entity?
- What is the packet size?
- Are they simple transaction (like bank exchanges) data exchanges, or do they contain rich state data that contains large amount of contextual data?
- Have all the entities joined the execution before publishing data or do they join bundled/ad-hoc?
- Are there filters in the system managing data flow?

The point here is that once designers invite complexity in to the network design there is a tendency for the effects to spill over in to other areas that may or may not be anticipated.

Fortunately the M&S community has a great deal of experience in addressing many of these issues. This has resulted in the development of ways to mitigate these challenges. The three primary areas are the use of standards, tools, and processes.

Standards

Standards provide an agreed way of doing something. Both DIS and HLA are internationally recognized standards for the design and exchange of simulation data elements. By employing sets of standards the network designers can predict how data will flow, what needs to occur in the translation of that data, and be confident in the validity of the data exchange outcomes. Ultimately the practice of using recognized standards should result in reducing both risk and cost.

With the experience of employing M&S standards and thousands of hours of using the simulations to support events that include training, testing, and planning the community has developed a number of tools. These tools assist in network design and data exchange. When used, the tools provide an ability to improve the quality of data exchange, limit error, and provide reliable technical capabilities. The US Defense Modeling and Simulation Coordination Office has long supported the development and use of tools that target M&S interoperability. Two important products coming out of that support are:

FEAT – The Federated Engineering Agreements Template (FEAT) benefits developers, managers, and users of distributed simulations by providing a well defined and easily read (human and machine) format for recording agreements about the design and use of the distributed simulation. The template also benefits this community by enabling the development of federation engineering tools that can read the schema and perform federation engineering tasks automatically (SISO, 2013, p. 2).

Gateways - Gateways are protocol translators developed for distributed simulations. They provide for interoperability among different types of simulation architectures. There are versions of gateways that convert the Distributed Interactive Simulation (DIS) protocol to High Level Architecture (HLA) Run-Time Infrastructure (RTI) service calls, and vice versa. While there is no recognized standard for the design of gateways they are recognized tools and today's M&S multi-architecture networks could not function without their use (Fig 4).

System Engineering Processes

In addition to the tools there are also system engineering processes in place which provide a consistent and stabile environment for the design of M&S networks. The application of processes is also an excellent way to reduce risk as their application will, at the very least, help ensure the most significant factors of the design are accounted for. One point that is not inherent in using a process but is a frequent point of failure, especially when there is a requirement to replicate the design, is record keeping. Often the design record is little more than personal knowledge of the people involved and their notes. Therefore it is critical that some form of official records be captured and maintained. The earlier mentioned FEAT is one method of having a transcript of how the network was designed.

Two of the processes that are widely used are also recognized standards. There is the IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP) and the Distributed Simulation Engineering and Execution Process Multi-Architecture Overlay (DMAO).

DSEEP - *This recommended practice defines the processes and procedures that should be followed by users of distributed simulations to develop and execute their simulations; it is intended as a higher-level framework into which low-level management and systems engineering*

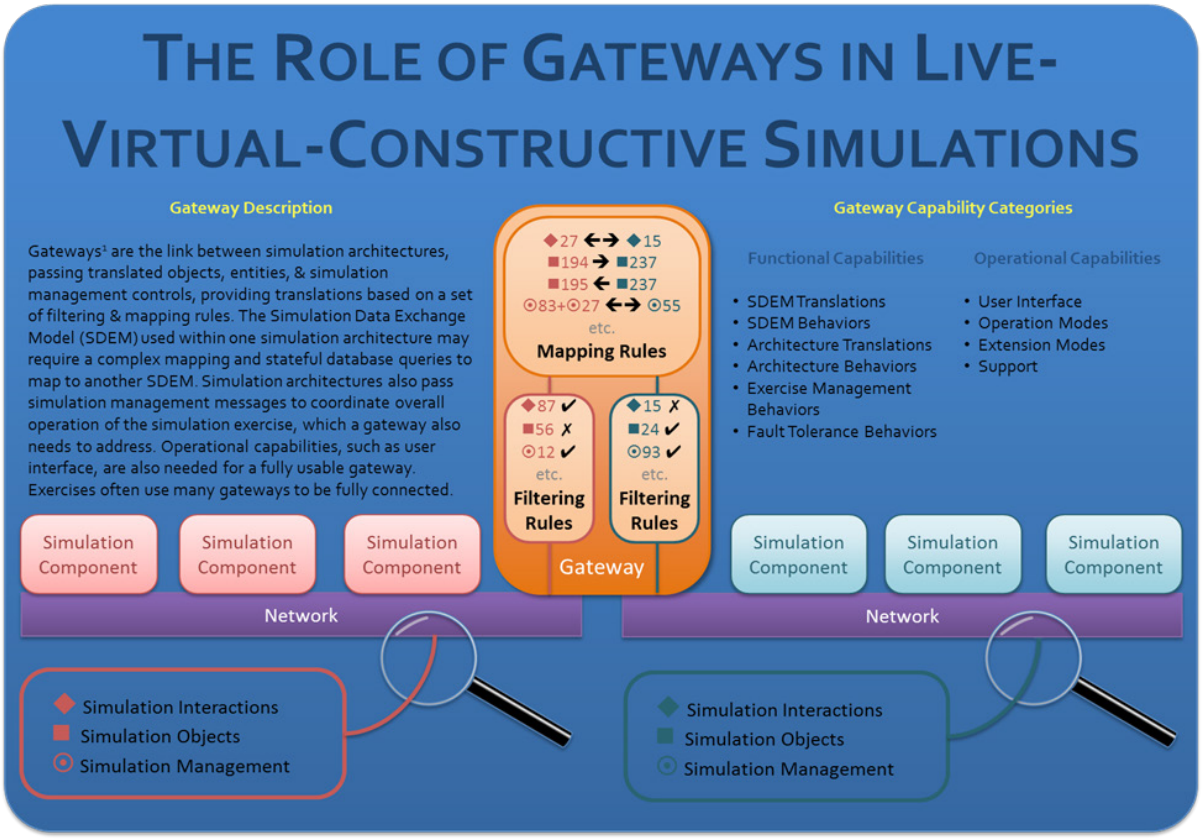
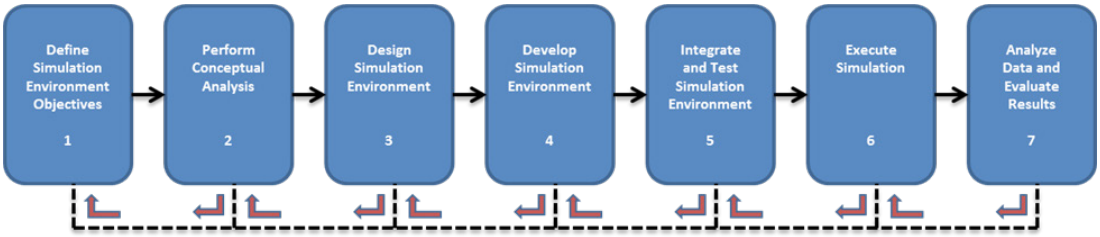


Figure 4 – Gateways



Distributed Simulation Engineering and Execution Process (DSEEP) top-level process flow view

practices native to user organizations can be integrated and tailored for specific uses (IEEE, 2011).

DMAO - *The DSEEP Multi-Architecture Overlay (DMAO) (IEEE Std 1730.1) is intended as a companion guide to the DSEEP (IEEE Std 1730™-2010).1 The simulation environment user/developer should assume that the guidance provided by the DSEEP is applicable to both single- and multi-architecture developments. The DMAO provides the additional guidance needed to address the special concerns of the multi-architecture user/developer* (IEEE, 2013).

Conclusion

In this paper the terms 'system' and 'complexity' have been used repeatedly. Both of those terms are represented by bodies of research covering System Theory and Complex Systems Theory. The use of these terms in this paper is not intended to imply that this is a contribution to those bodies of knowledge but rather the point of this paper is to highlight aspects of M&S design that can either intentionally or unintentionally be made more difficult through the combination of architectures that were not designed to work in unison. The lesson here is that if the designers want an artificially contrived network to function they will have to force it to do so.

In closing the following recommendations are offered. First, the designers should question the need for combining M&S architectures. By asking the question, 'Do we really need to do it this way?' brings out a need to look at what is driving the requirement. What are the technical reasons for combining architectures? Is there a situation where certain models or simulations will only

function in specific environments therefore we need to combine the architectures or is the effort being driven for the sake of technology. Otherwise stated as; we are making the design complex because we can. Second, whether the design calls for a single architecture or the combination of architectures the designers should work with recognized standards. This limits risk and cost because you are working with reliable systems. There is a false belief that restricting the use of standards restricts innovation. It isn't standards that restrict innovation but rather it is designers that will only accept doing things a certain way that restricts innovation. By way of comparison, all of the parts in a Tesla automobile meet some internationally recognized standard yet these cars represent some of the most innovative designs of the last 50 years. Third, keep good records. Setting up an M&S network should not be for a onetime use. It is through these records that designers can not only replicate a successful design but also find ways to improve and apply innovative solutions to make future use more efficient and cost effective.

Complexity, in and of itself, is not necessarily a negative concept but where possible M&S network design benefits by not inviting more. Following the recommendations given will help avoid that situation. ■

RERERENCES

[1] Characteristics of Data Quality. (2015). Retrieved from quizlet.com https://quizlet.com/13806017/characteristics-of-data-quality-flash-cards/.

[2] Data Characteristics. (2015). Retrieved from Wikipedia http://en.wikipedia.org/wiki/Data.

[3] Lessmann, Kurt. "Re: Any recent CTIA experience." Message to the author 9 MAY 2015. E-mail.

[4] Linthicum, D. (2009, February). *Identifying Data Characteristics for Data Integration.* http://www.ebizq.net/blogs/linthicum/2009/02/identifying_data_characteristi.php.

[5] IEEE Standards Association. (2011). *IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process (DSEEP)*. New York, NY: IEEE.

[6] IEEE Standards Association. (2013). *IEEE Recommended Practice for Distributed Simulation Engineering and Execution Process Multi-Architecture Overlay (DMAO)*. New York, NY: IEEE.

[7] IEEE Standards Association. (2012). *IEEE Standard for Distributed Interactive Simulation – Application Protocols*. New York, NY: IEEE.

[8] IEEE Standards Association. (2010). *IEEE Standard for Modeling and Simulation (M&S) High level Architecture (HLA)-Federate Interface Specification*. New York, NY: IEEE.

[9] Representation term. (2015). Retrieved from Wikipedia http://en.wikipedia.org/wiki/Representation_term.

[10] SISO. (2006). *Base Object Model (BOM) Template Specification*. Orlando, FL: SISO.

[11] SISO. (2013). *PDG Name: Federation Engineering Agreements Template (FEAT)*. Orlando, FL: SISO.

ABOUT THE AUTHOR

Gary W. Allen, PhD

Deputy Director
Instrumentation Training Analysis Computer Simulations and Support
US Army Europe - Joint Readiness Multinational Center
Hohenfels, Germany

Dr. Gary W. Allen has worked in various aspects of modeling and simulation for the past 30 years and is a DOD Level III Acquisition Project Manager. He is currently the Deputy Director for the Instrumentation Training Analysis Computer Simulations and Support (ITACSS) at the US Army Joint Multinational Readiness Center, Germany.

As a career US Army Military Intelligence Officer has hands-on experience with formulating intelligence from varied information sources and presenting that to command decision makers.

He was a member of the team that founded the Training Simulation Center for I Corps at Ft. Lewis, Washington (1980), Director of the Simulation Training Branch at the US Army Intelligence Center and School, Ft. Huachuca, AZ (1989-1992)

Project Director for the TACSIM Intelligence Simulation, and part of the design group that initiated the Aggregate Level Simulation Protocol (ALSP).

From 1996 – 2008, he was the US Army Liaison Officer to the German Military Research and Development Agency in Koblenz, Germany responsible for seeking out international S&T solutions for US Army requirements.

Dr. Allen led a successful effort as Project Manager for the DoD High Level Task, "Live, Virtual, and Constructive Architecture Roadmap Implementation" project (2009-2014) and initiated the ongoing Cyber Operations and Training Simulation (COATS) Project.

US representative to numerous international study groups to include NATO and TTCP working to apply latest M&S technologies to coalition requirements.

Past Technical Advisor to the NATO Modeling and Simulation Group (NMSG)

As the Deputy Director of the Instrumentation Training Analysis Computer Simulations and Support (20014-2015) Dr. Allen guided a team that supplied a world class L-V-C training environment in Europe.

His academic background includes MS in Telecommunications Systems Management, School of Engineering, University of Colorado (Boulder), and PhD in Instructional Technology, University of Kansas (Lawrence). Dr. Allen is a member of the Phi Kappa Phi National Honor Society, a 1999 graduate of the Army War College, and is a DOD Acquisition Corps Level III Certified PM. Dr. Allen currently lives in Germany and devotes some of his time to teaching and consulting on international M&S projects.

WE WORK FOR YOUR BUSINESS.

Is your organization currently facing a challenging Information Technology oriented research and development problem that you need to have addressed in a timely, efficient and cost effective manner?

HOW CAN THE CSIAC HELP?

In a time of shrinking budgets and increasing responsibility, IACs are a valuable resource for accessing evaluated Scientific and Technical Information (STI) culled from efforts to solve new and historic challenges. In addition, users can leverage the CSIAC's experienced technical scientists, engineers, and information specialists to answer their technical questions.

We provide expert technical advice and assistance to our user community. CSIAC is a competitively procured, single award contract. The CSIAC contract vehicle has Indefinite Delivery/ Indefinite Quantity (ID/IQ) provisions that allow us to rapidly respond to our users' most important needs and requirements.

CALL NOW! 800-214-7921

EMAIL at: info@csiac.org

Technical Inquiry Services

The CSIAC provides up to 4 hours of Free Technical Inquiry research to answer users' most pressing technical questions. Our subject matter experts can help find answers to even your most difficult questions.

Core Analysis Tasks (CATs)

Challenging technical problems that are beyond the scope of a basic inquiry can be solved by initiating a Core Analysis Task (CAT). Through the CAT program, the CSIAC can be utilized as a contracting vehicle, enabling the DoD to obtain specialized support for specific projects within the CSIAC's technical domains (Cybersecurity, Software Engineering, Modeling & Simulation, and Knowledge Management/Information Sharing).

FOR MORE INFO, GO TO: https://www.csiac.org/about/technical-inquiries-and-cats

Computer Supported Training Solutions: Discussion of a New Framework for Effective Development and Deployment

Dr. Amela Sadagic
Naval Postgraduate School

Maj Matthew C. Denney
USMC (Ret)

The potential that computer supported training solutions bring to the military training domain is fairly well recognized, yet we still do not see evidence of large scale adoption or effective deployment of these systems in military forces' training practices. The opportunities these solutions offer consist not only in the precious resources they may save (material, logistics, human labor), but also in the training opportunities they provide, which would not be available or even possible otherwise. It is, for example, only by the use of simulations that a Fire Support Team can practice Call for Fire and employ multiple air and ground assets whenever they need to; the same level of training flexibility simply could not exist if the Fire Support Team were to use real military assets and resources. While it is important to recognize that computer-supported training solutions do not represent a panacea and they will not be the most effective solution for all training situations, it is very likely that in the future they will have a more important role in supplementing the training needs of the military than they do today [1][2].

Good solutions do not happen by chance in any domain – they are the result of long-term, continuous and focused efforts by parties that have a vested interest in that domain. Current investments directed towards developing and fielding computer supported training solutions are not insignificant; several specialized agencies are engaged in securing and managing funds aimed at supporting both basic and applied research opportunities, and other agencies organize and regulate the fielding of new systems and the maintenance of already deployed training solutions. At the same time a number of research teams are involved in designing new technologies and new training methodologies – an effort that is expected to be the basis for future advancements in the domain of computer supported training solutions. The user community is also engaged in this process in its own ways: users try out different systems and help in identifying the needs and selecting the solutions that support their work most effectively, while also acquiring invaluable insights during the actual long term use of these systems (Figure 1 shows young USMC service members using Close Combat Marines (CCM), and Figure 2 shows a virtual Kilo2 training range that served as a basis for a user study focused on novel learning and training strategies in support of urban warfare training).

Our extensive knowledge and detailed insights about the various elements that play a significant role in this domain, and our long experience in working with sponsors, researchers and users, made us realize that many facets of this effort could be improved and executed in a way that would provide a better guarantee for reaching the desired results. Our past combined work and expertise, a series of focused research projects (examples: VIRtual Training and Environments (VIRTE) and "Behavioral Analysis and Synthesis for Intelligent Training – BASE-IT" [3], both sponsored by the Office of

Naval Research (ONR)), as well as our work on collecting and analyzing the data that reflect the acquisition and use of computer supported training solutions in USMC domain [4][5], helped us refine the approaches presented in this text. We elaborate on current practices as seen from the users' and researchers' perspective, and propose a set of recommendations and guidelines in support of a new framework for more effective approaches and partnership efforts between major participants in this domain.

Figure 1: Close Combat Marines (CCM)

Figure 2: Virtual Kilo2

Users' Perspective: Current Practices

The user community provides input and gets engaged in developing and acquiring computer supported training solutions in several ways. One way in which those solutions get developed is when the user community identifies a need and creates the Universal Needs Statement (UNS) that is submitted up the operational chain of command. Upon approval, the requirement is given to Marine Corps Systems Command's (MARCORSYSCOM) PMTRASYS. This process, for example, is how the High Mobility Multi-purpose Wheeled Vehicle Egress Assistance Trainer (HEAT) was developed and fielded to the various Marine Corps Bases. A different approach was used to develop the Deployable Virtual Training Environment (DVTE); much of this suite resulted from research efforts funded by the Office of Naval Research. In this effort both university and corporate research teams involved many users in several different ways: they were part of a task analysis effort, they acted as Subject Matter Experts in consultations and system evaluations, and they also took part in user studies. The prototypes were then 'productized' to make them robust and ready for actual use. Other elements of the DVTE suite were purchased and added to the set, and the entire suite was fielded to USMC bases. A completely different option for adoption of training solutions is through industry development and demonstration at trade shows, such as the Interservice/Industry Training, Simulation and Education Conference (I/ITSEC) where technology demonstrations and subsequent purchases take place.

Funds used to develop the systems are meant to do just that – support the development phase. Another type of funding – support funding - is used for maintenance of the current version of adopted systems and for contractor support. As Tactics, Techniques and Procedures (TTP) change and new operational systems are fielded, there is rarely a process to identify and/or fund the modifications that are required to keep already fielded training systems current. There are additional issues that negatively influence the effectiveness of these solutions, and we list here only a few of the most significant ones. (1) Systems are typically fielded without having progressive scenarios (crawl, walk, run), (2) Documentation consists of a technical manual, at most, but no manual that would have tested advice on how to use the system most effectively in training practice, (3) Systems do not come with the unit assessment methods that would help evaluate the effectiveness of training solutions used by a given training audience, (4) Job descriptions for contractor support personnel include requirements for relevant experience, but contract documents have no advice or requirements for a process through which support personnel would maintain currency with the evolving operational environment, (5) System interoperability is frequently not requested in the UNS, resulting in situations such as that with the Supporting Arms Virtual Trainer (SAVT), which was not designed to be compatible with aircraft simulators that could "fly" Close Air Support (CAS) missions to support Tactical Air Control Party (TACP) training, (6) Government Acceptance Tests (GAT) focus only on system performance, not on user performance, (7) A full Verification, and Accreditation (VV&A) is requested [6] yet it is rarely conducted, (8) Most systems are not tested for their training effectiveness prior to their deployment. Consequently it is very hard for PMTRASYS to know if users will actually benefit

from using the fielded systems prior to their fielding. In addition, post fielding user surveys are rarely conducted. The result of these and other similar issues is that training forces are very reluctant to supplement, let alone replace their current training approaches by introducing computer supported training solutions.

Researchers' Perspective: Current Practices

A number of research teams are actively involved in research efforts that indirectly or directly benefit the military training domain. Many of these efforts are focused on computer supported training solutions, most specifically different types of simulators, simulations and game-based systems, as well as sensor technologies and systems on instrumented training ranges. Any engagement in the military domain requires a level of understanding of the domain that goes beyond the information found in military documents and manuals. Due to limited funding and infrequent opportunities for the research teams to visit military bases and spend time observing current training practices extensively, some teams' knowledge about the subjects of their investigations are not at the level that is optimal for their research. Even when teams are able to make those visits, they are very often of a short duration with few opportunities to conduct long interviews and have repeated visits and access to the same units. The ability to fully understand the needs of users and then to make critical connections with the current or future technologies is paramount if a desire is to design and develop the best solutions. Additionally, it is equally important to understand the underlying conditions under which the military acts in the training domain, and learn more about actual experiences and system of values they hold in given domain [7][8].

Similarly, a good number of user studies that are focused on evaluating the effectiveness of proposed training solutions are done using 'convenience subjects' (typically colleague students) instead of having actual domain users, i.e. active duty military, who have the type and level of expertise needed in user studies. Even when domain users do get engaged in the studies, their number is usually very small (studies with a large number of subjects are quite rare), the exposure time to novel training treatments that are being tested is also not long enough to draw highly reliable conclusions, and even time when they are exposed to training (study) conditions may not be the optimal one (users exposed to training situations that do not correspond to their proficiency level). We have also observed a tendency to have a large number of small studies, where each study focuses on a fragment of the larger issue or system; at the same time there are very few efforts focused on providing tested advice on how all those results should be integrated in a coherent system that would ensure comprehensive support of a full spectrum of user needs exhibited in some operational environment.

The Way Ahead: Elements of Proposed Framework

A critical component of success for any complex undertaking lies in a well selected and well connected set of elements of the general framework that all participants in the process support and observe. We provide here a list of recommendations for the most prominent elements of a proposed Framework for Computer Supported Training Solutions in the military training domain. Examples and discussions provided in this text take as an example the US Marine Corps (USMC) domain, however they are very much applicable to situations and institutions or other services and DoD in general.

Comprehensive knowledge about training audience, conditions, objectives and standards: Before a specific technical solution is even proposed, a clear identification of the training audience and its characteristics; training objectives; descriptions of the environment and conditions under which those tasks are to be performed; skills, knowledge, performance standards, expectations and the level of expertise to be gained; identified training gaps; future (projected) training needs; users' value system, concerns and priorities should be established and defined, as well as skill retention rate and decay. The usability tests and tests of training effectiveness done later on should be conducted using these same parameters and requirements. We also advise acquiring detailed understanding about characteristics of the users - their interests, attitudes, expectations, technical skills, and personal ownership of digital devices, to name a few. The latter one provides clear insights about users interests, motivations, but also the untapped skills they posses, and possibly the expectations they may have from their work environment. Today's users are unlike any other group in the past - a good illustration of characteristics of this community was derived in study organized in Summer 2013 [4][5] that identified young Marines as the owners of three digital devices - a smartphone (90.91%), game console (78.64%) and laptop/desktop computer (73.18%), with internet connections in their rooms (81.36%), and being avid users of social networking sites (Facebook - 90%), email (85.90%), and first person shooter games (77.27%) (Figure 3).

Domain support for research efforts: All research projects, especially the ones categorized as *applied research*, require extensive consultation with subject matter experts (SMEs). The military community (sponsors, transition customers, base leadership) should make additional efforts to ensure that research teams do get access to a variety of information sources and get opportunities for consultations with the SMEs. We also see the need for extended relationships between the research team and SMEs/practitioners – in order to create true partnerships. This approach enables additional dimensions of the research effort: the interaction and collaboration between researchers and practitioners allows for easier and more direct integration of project results into the community of training providers and end users. The connections, trust and credibility built in that collaboration will the important factor in adoption process. If domain practitioners are given an opportunity to be partners in the project and recognize themselves as co-owners of the process or the results of that work, they are more likely to adopt the results and promote the values of that effort afterwards. Likewise, the same long-term collaboration gives researchers a unique opportunity to have closer insights in the extensive expertise of practitioners, which maximizes the probability of achieving highly valuable and relevant results in their own work.

Work with domain (expert/end) users: If the research studies need to involve a specific user population, the military community should invest maximum efforts to ensure that research teams get

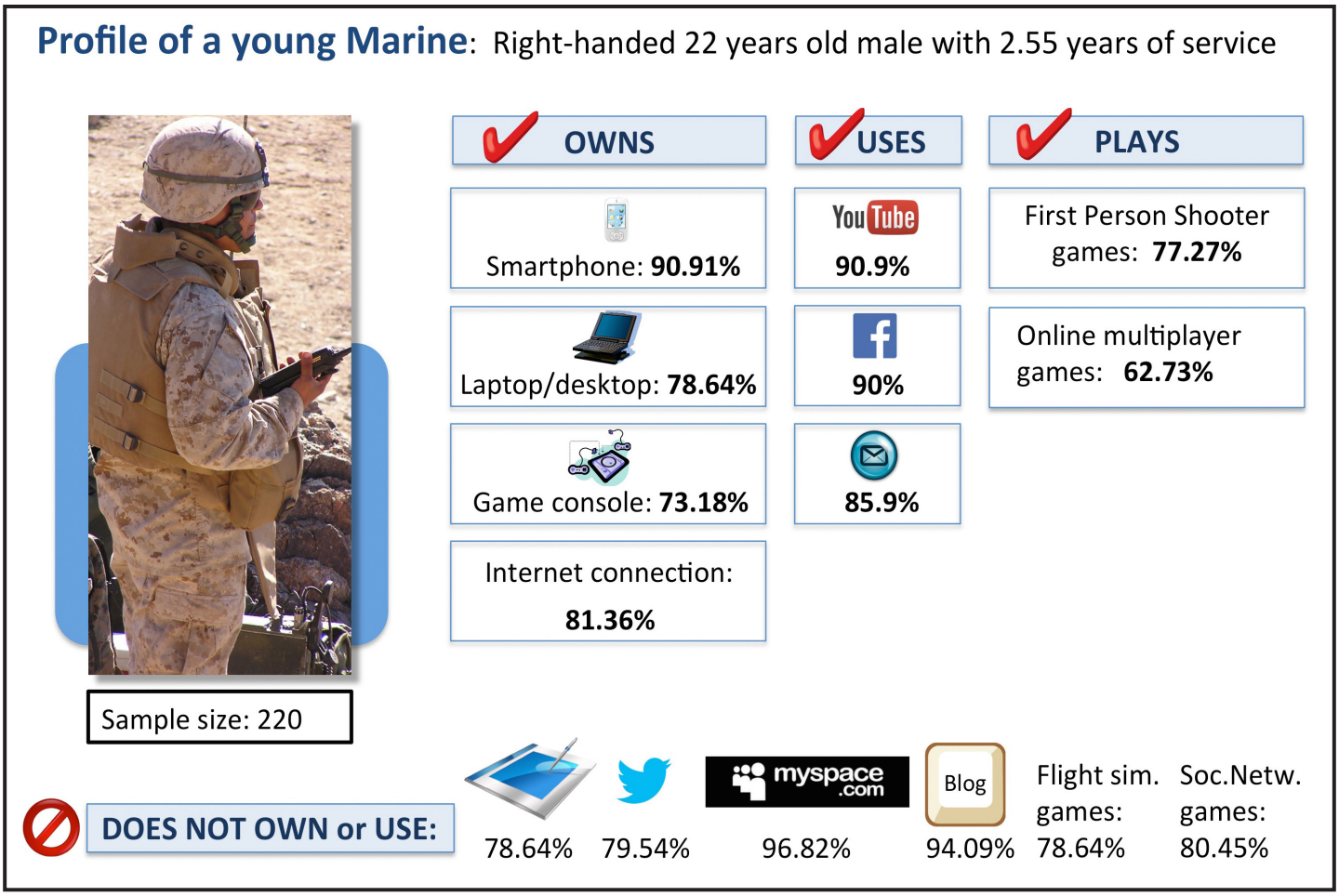


Figure 3: Profile of a young Marine [4]

access to domain (expert/end) users. This is a necessary condition to ensure that the results obtained in the studies are indeed relevant to the training needs and characteristics of a targeted user population. In addition to engagement of domain users in larger user studies, there is a need to also embrace and support smaller scale tests of prototype solutions – this is the only way in which different solutions can be perfected over the time and have a better chance to be widely deployed at the end of their development and testing cycle.

Recognition and support of systems interoperability: Those responsible for the development process methods, Universal Needs Statement (UNS), research projects and trade show purchases, must be made aware of the needs for interoperability before the actual products are made or purchased. They should be familiar with the requirements for true interoperability if some solutions need to exist and work in concert with other solutions. For example, PMTRASYS has adopted the Army's Common Training Instrumentation Architecture (CTIA) that standardizes the components of that system. At the basic level this means that all solutions will have to co-exist in each other's space - if one buys a target system from one company, a controller from another company has to be able to operate that same target and not require the purchase of another target system. Similarly, all graphical simulations and their 2D viewers must support a common mapping system. This requirement will ensure a basic level of compatibility and interoperability. A second modification should be the requirement that development and purchasing follow the Joint Capabilities Integration and Development System [9], or JCIDS acquisition process as well as inclusion of the Marine Corps Operational Test and Evaluation Activity (MCOTEA) [10]. While the UNS submitter, research team or purchaser may not require system connectivity but Training and Education Command (TECOM) does, the initial requirement should be modified to align with the TECOM requirement. Operational systems (weapons, computer command system, etc.) are developed to support the Combatant Commander's Contingency Plans (responses to potential crisis), so training systems should be developed to support a TECOM Training Plan.

System development and deployment: What does it include and who is responsible? Fielding systems to bases is sufficient for contract and maintenance support, however for the system to be most effectively utilized by the training audience, a TECOM Formal Learning Center (FLC) is ideal to be the system proponent, responsible for both development and post fielding support. It is recommended that the system and the contractors who support its operation become the responsibility of the FLC. It is also recommended that the FLC actively participate in the GAT to ensure that the system provides proper training prior to fielding. FLCs have processes identified in the Systems Approach

to Training (SAT) manual to include Learning Analysis and, Learning Objective Development which assist the instructor staff in developing instruction, training and evaluation. The same documents would prove useful in training system development. For example, the DVTE Combined Arms Network would allow an aircraft to fly through an active artillery trajectory without alerting the users; that same activity and situation would not be allowed by the Expeditionary Warfare Training Group's (EWTG) Fire Support Coordination Course. If the EWTGs had been involved in the development of DVTE from the beginning, this inconsistency would most likely have been avoided.

Certification of instructors (contractors): It is our firm belief that all individuals who provide instructions with any training system, including computer supported training systems, should go through regular certification and recertification processes – this also applies to contractors who operate the systems or provide instructions. Their level of expertise and readiness should be subjected to the same level of scrutiny imposed on any professional performer in the service. Additionally, the responsibility of each instructor (contractor) should not end with providing the instructions – they should also actively look for any instance of negative training transfer that may occur, even if such trends were not initially registered in the system. For example, a DVTE operator, certified by an EWTG, would identify the conflict with the aircraft flight path and the artillery trajectory if the system (in this case DVTE Combined Arms Network) was incapable of doing so.

Fielding the systems: In an ideal case the system should be fielded with a library of tested progressive scenarios and assessment forms just as if the system was part of the curriculum. Users should be requested to provide a feedback to the FLC through a well-established mechanism, a version of the Instructor Rating Form. This process should be required by the SAT manual. The FLC would then include the utilization of the system in their Course Content Review Boards (CCRB) where the FLC and operational units regularly review and revise the curriculum. Supervisor and Graduate Surveys, and other sources of feedback for system users and supervisors would, as well as the CCRBs, ensure that these systems continue to provide necessary and valued training.

Comprehensive support for large scale deployment and adoption of training solutions: Large scale adoption and use of some training solution by all (or almost all) members of training community is needed when that group decides to adopt qualitatively different way of accomplishing that task, with objective to achieve better training results and to support training situations that are not possible with other means. Those were the very reasons why today all pilots, for example, use flight simulators in their training. The hard lessons that we learned from our extensive engagement in a domain of computer supported training simulations, suggest that a success of the adoption of novel technology does not and cannot be left alone and unattended. The expectation that people and institutions will recognize the value of novel technology on their own, and that the large scale adoption of that technology will follow, regularly remains to be only the expectation - considerable efforts on promotion, demonstration of values in and by peer community, strong communication channels and supporting infrastructure is needed if a full success is to be reached [11][12] [4][5]. A number of factors that influence adoption of training solutions range from technical characteristics of those systems, human factors (usability, user acceptance and attitudes), leadership endorsement and support, communication channels used to promote the solution in military community, human network (user community) and active engagement of a larger number of agents of change and their aids to support a spread of ideas and adoption, to elements of training domain being well resolved (existence of full training package - having a training solution/system and tested advice how to use it effectively, easy access to training solution and unlimited number of training opportunities unrestricted by location and time, good throughput, train-the-trainer program, more active and changed role of simulation centers (distributing their expertise across the units), introducing challenge programs and competitions, diverse set of 'push' strategies instead of relying on 'pull' approaches, etc) [4][5].

Harnessing the experiences and insights of users: Once a system gets fielded, users acquire invaluable insights through long-term use; their experiences could be of great value to both system makers and to research teams. It is our understanding that this experience-based knowledge rarely if ever gets reported or utilized, and issues that could have been addressed in new solutions, remain unexamined and unimproved. Ideally, the SAT manual should either require this long term review process for training systems used at FLCs (in addition to the currently required review of instructional material) or PMTRASYS should partner with the Marine Corps Center for Lessons Learned System (MCLLS) to gather data on training systems much as MCLLS gathers data on operational systems.

Conclusion

We believe that the approaches proposed in this text provide a valuable starting framework and a set of general guidelines for more effective design and deployment of computer-supported training solutions not only in USMC but also in other services and DoD in general. Some approaches that we discussed in this text support long-term processes that extend well beyond the cessation of initial project activities. The long-term benefits of efforts directed towards promoting system self-sustainability, interoperability and on-going improvements, are even more important in situation where funding for research activities and development of training solutions is increasingly limited. We hope is that our suggestions can serve as a catalyst in a discussion organized by all parties who have vested interests in the domain of military training. ■

Acknowledgements

The authors would like to acknowledge our project sponsors and many USMC units who volunteered their time to participate in our user studies. The opinions expressed here are those of the authors and do not necessarily reflect the views of the sponsors, the USMC or the Department of Defense.

The Defense Office of Prepublication and Security Review (DOPSR) has reviewed/cleared this document for public release (Case No. 16-S-1860).

REFERENCES

[1] Naval Science & Technology Strategic Plan, Office of Naval Research (ONR), Sep 2011.

[2] Marine Corps Science & Technology Strategic Plan, Jan 2012.

[3] Sadagic, A., Welch, G., Basu, C., Darken, C., Kumar, R., Fuchs, H., Cheng, H., Frahm, J.M., Kolsch, M., Rowe, N., Towles, H., Wachs, J., and Lastra, A. (2009). New Generation of Instrumented Ranges: Enabling Automated Performance Analysis. Proceedings of 2009 Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC-2009), Orlando, FL.

[4] Yates, F. A. (2013). Diffusion and Large-scale Adoption of Computer-supported Training Simulations in the Military Domain (NPS Master Thesis) Sep 2013. Available from NPS Calhoun database.

[5] Sadagic, A. and Yates, F. (2015). Large Scale Adoption of Training Simulations: Are We There Yet? I/ITSEC 2015 conference, Nov 30th-Dec 4th 2015, Orlando, FL

[6] DoDI 5000.61 (2009). DoD Modeling and Simulation (M&S) Verification, Validation, and Accreditation (VV&A)

[7] Sadagic, A., and Darken, R. (2006). Combined Arms Training: Methods and Measures for a Changing World, NATO workshop Virtual Media for Military Applications, US Military Academy, West Point, NY, 13-15 June 2006.

[8] Zachary, W., Hoffman, R. R., Neville, K., and Fowlkes, J. (2007), Human Total Cost of Ownership: The Penny Foolish Principle at Work, IEEE Intelligent Systems, March/April 2007.

[9] CJCSI 3170.01H, Joint Capabilities Integration And Development System

[10] MCO 1553.3A, Marine Corps Order 1553.3A

[11] Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, Volume 13 Issue 3, p. 319–339

[12] Rogers, E. M. (1995). Diffusion of Innovations. New York, NY: Free Press, 4th edition

ABOUT THE AUTHORS

Dr. Amela Sadagic

Naval Postgraduate School

Dr. Amela Sadagicis a computer scientist and a Research Associate Professor at the Naval Postgraduate School (NPS), Modeling Virtual Environments and Simulation (MOVES) Institute, Monterey, CA, with 29 years long professional research career. She has been a PI and co-PI on many research efforts done at NPS; the research efforts were supported by close to $10M of funding and involved over 4500 USMC and USN personnel as subjects in user studies. In the past she was a Director of Programs at Advanced Network and Services Inc. where she designed and led the programs focused on the use of emerging technologies in learning. She was also responsible for coordination of a research consortium "National Tele-immersion Initiative (NTII)" that involved 30 researchers from leading US universities, who worked on the first 3D tele-immersive system over Internet2. Her expertise and research interests include: simulations; Virtual Environments; human factors and presence in VE; human subjects studies; evaluation of learning and training effectiveness in computer supported environments; multiuser collaborative environments; game-based systems; coupling of emerging technologies in support of systems for operation, training and learning; acquisition and large scale adoption of technical innovations. Dr. Sadagic holds PhD degree in Computer Science from the University College London, UK.

Maj Matthew C. Denney

USMC (Ret)

Matthew C. Denney (USMC, Maj. Retired) was an infantry officer with multiple instructor tours, to include the Tactical Training Exercise Control Group (TTECG) at the Marine Air Ground Task Force Training Center. At TTECG he was responsible for exercise design, control and assessment for live fire training from platoon to battalion level as well as instructor certification and the integration of emerging technologies. Upon retirement he worked at the Marine Corps Systems Command Program Manager for Training Systems on assessment and integration. He currently works at the Marine Corps Mountain Warfare Training Center providing Combat Operations Center, Fire Support Coordination Center and Fire Support Team training, Command and Control Systems training and Constructive unit support to Mountain Exercise.

Back to Basics: Firmware in NFV Security

Daksha Bhasker
Bell Canada

Carriers no longer want their speciality pizzas delivered in a box, fully baked with pre-determined toppings. In fact they figure that it is economical to purchase standard pizza ingredients wholesale, bake ginormous crusts and believe they can please their customers faster by delivering custom toppings by slice on demand.

Network function virtualisation (NFV) effectively takes carriers out of the "pizza" box by dismantling the content of numerous proprietary devices and classic network appliances into their rudimentary components: software, compute, storage and network. This effectively blows open the carriers box based security architectures, perimeters and controls. Carriers need to monitor the integrity of resources as physical server firmware, hypervisors, guest operating systems to ensure customers' sensitive data is secure on their cloud. This brings carriers to rethink forgotten threat vectors on the redefined, yet age-old attack surface that will dominate and pervade the high volume commodity infrastructure: Firmware.

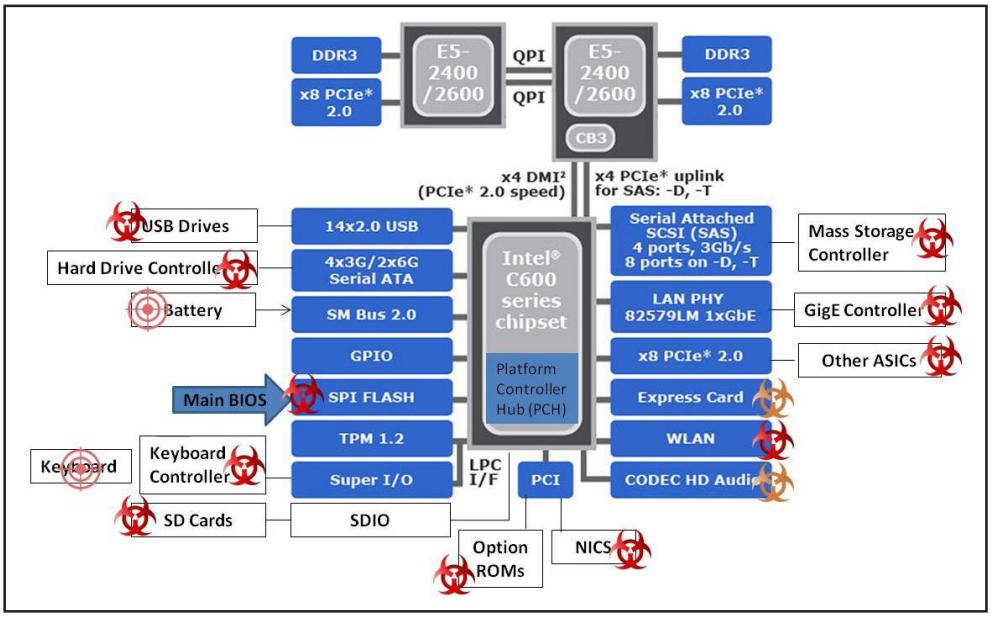


Figure 1: [1] [2]

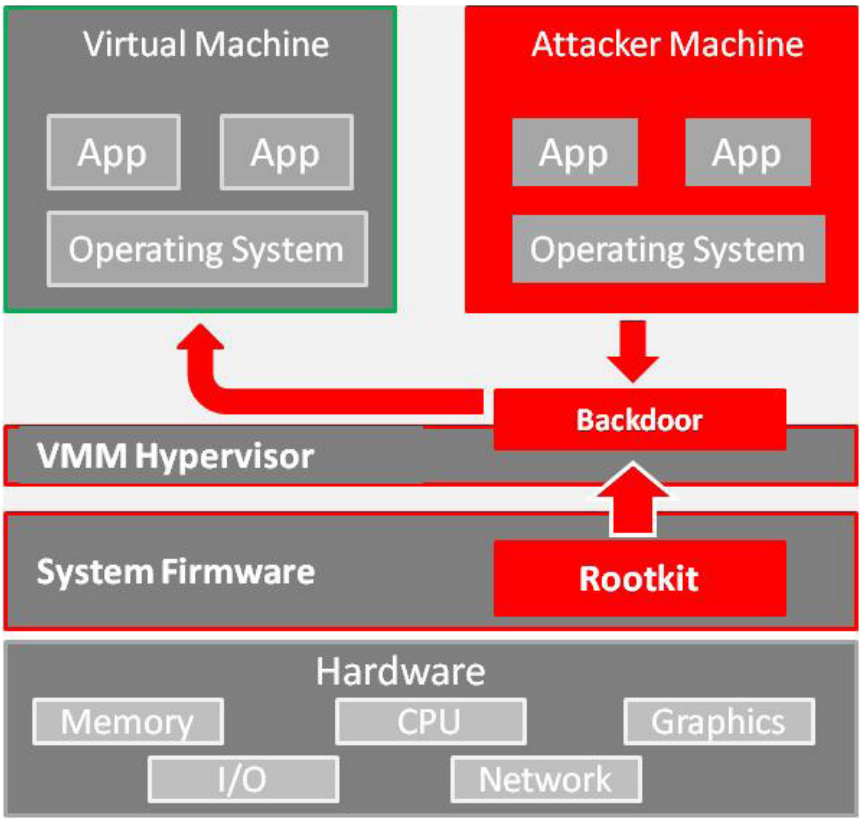


Figure 2: [6]

Firmware is the first code run by a system and is typically written on read only memory (ROM) chips soldered onto circuit boards ranging from BIOS chips on the motherboard to controller chips of peripheral devices. Unified extensible firmware interface (UEFI) is a more generic type of computer firmware standard, invoked during the boot process in newer systems. Firmware can be found on USB drives, hard drives, keyboards, SD cards, RAID controllers, SSDs, network cards, video and audio cards among others. Almost every electronic device today has rewritable firmware chips. Embedded software/ firmware in field programmable gate arrays (FPGA), application specific integrated circuits (ASIC), application specific standard products (ASSP), system on a chip (SOC) and firmware embedded systems are widely found throughout every industry.

In recent times there has been a resurgence of firmware attacks. Firmware malware is persistent, not easily detected and can typically be removed only by manually re-flashing the chip. The recent Synful knock attack installed a back door by modifying Cisco router firmware affecting the Inter-networked operating system (IOS) of Cisco 1841, 2811 and 3825 routers [3]. Once infected, an attacker has unrestricted access, can install various functional modules in the router from the anonymity of the internet that could compromise availability of other hosts as well as enable access to sensitive data in an organisation [4]. Earlier this year white hats announced a firmware worm for Macs called thunderstrike that can be deployed remotely [5]. The worm exploits UEFI or BIOS vulnerabilities giving an attacker physical access to a computer and replicates itself through shared thunderbolt devices. Firmware attacks are surfacing more frequently, and methods for infecting and propagating firmware attacks, continue to evolve. Figure -1 depicts the various firmware that can be targets for malware or attacks in a x86 chip on a typical enterprise blade server.

In the NFV environment, physical devices such as firewalls, load balancers, routers or other traditional devices become software applications residing in virtual machines (VM). When a rootkit is implemented, or the system firmware compromised, it can cause VM escapes [6]. This means a VM and its application no longer stay within the isolated containment of its guest operating system but can interact with or attack other virtual machines and host operating systems (Figure 2). In NFV deployments, a firmware vulnerability on a single manufactures' chip can expose and compromise large segments of infrastructure and networks. In the example above where the impact of the compromised Cisco routers were limited to the proprietary physical devices, models 1841, 2811

and 3825, in NFV environments, these same routers would be software based virtual routers or virtual network functions (VNFs) residing on virtual machines on commodity x86 hardware. Because of the ubiquity of the system firmware on commodity hardware, compromised firmware (Figure -1) would have a network segment wide impact, and not limited to infrastructure hosting specific router VNFs. Instead the impact would be felt regardless of the virtual network function hosted. Firmware vulnerabilities that were isolated by the confines of proprietary physical devices now have a broad network or data centre wide reach of exposure. The extent of impacts of exploited BIOS/UEFI and other system firmware vulnerabilities in NFV, raises firmware security up the list of security priorities into the spotlight.

In some ways, it is a return to the past, to dust off and reinstate, with new importance long forgotten security basics.

Be vigilant of your supply chain and ensure only manufacturer certified or authorised agents are sources and handle your equipment.

Software updates and patches for OSes and applications are a regular feature in most environments with vendors often pushing these patches over the internet to their customers. However, firmware updates and fixes, while released by most major OEMs, are typically not implemented with near as much diligence as software updates in most enterprises. OEMs release firmware patches for their newer hardware, while firmware vulnerability from a couple or more years prior may lay latent through the life cycle of the deployed hardware. In NFV environments it is of particular importance not to utilise infrastructure where the vendor has ceased to provide firmware updates. Additionally, it is imperative that firmware updates are included in routine corporate patch management practices.

Purchase hardware that have protection against malicious firmware modification. Some vendors are implementing CRC type checking routines that halt the execution of the BIOS if unapproved modification is made [7].

Notice the trusted platform module (TPM) chip in figure 1. Where the TPM chip is already present on the x86 hardware, consider using them. A TPM is a specification from the trusted computing group (TCG) that can perform cryptographic operations to protect small amounts of sensitive information to enable signing and measurements (hash values) that allows for a trusted boot process [8]. The TPM enables verification that the system boot utilised firmware that was not tampered with. TPM however is not a heavy duty cryptographic engine or accelerator, and hardware security module (HSM) may be considered for more robust security.

NFV is being deployed in clouds, in data centres, in vRAN in mobile edge networks, cloud based IoT management and data-analytics platforms, in general where volumes of infrastructure can be aggregated and operations optimised. In such aggregated environments, vulnerabilities have large domino effect and security by obscurity is not an option. The discussed measures for firmware security are not new however NFV has given them renewed value and a heightened security context. ■

Author's Note: Opinions expressed in this article are the author's and not necessarily those of her employer.

REFERENCES

[1] Intel, "server-chipsets," [Online]. Available: http://www.intel.com/content/www/us/en/chipsets/server-chipsets/server-chipset-c600.html. [Accessed 17 Oct 2015].

[2] X. Kovah and C. Kallenberg, "Are you giving Firmware Attackers a Free Pass?," in RSA, San Francisco, 2015.

[3] B. Hau, T. Lee and J. Homan, "SYNful Knock - A Cisco router implant - Part I," Fireeye, 15 Sep 2015. [Online]. Available: https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html. [Accessed 17 Oct 2015].

[4] K. Jain, "SYNful Knock - Backdoor Malware found on Cisco Routers," The Hacker News, 16 Sep 2015. [Online]. Available: http://thehackernews.com/2015/09/cisco-router-backdoor.html. [Accessed 17 Oct 2015].

[5] K. Zetter, "Researchers create first firmware worm that attacks MACs," wired.com, 3 Aug 2015. [Online]. Available: http://www.wired.com/2015/08/researchers-create-first-firmware-worm-attacks-macs/. [Accessed 17 Oct 2015].

[6] M. Gorobets, O. Bazhaniuk, A. Matrosov, A. Furtak and Y. Bulygin, "AttackingHypervisorsViaFirmware - Intel Security Threat Research," 6 Aug 2015. [Online]. Available: http://www.intelsecurity.com/advanced-threat-research/content/AttackingHypervisorsViaFirmware_bhusa15_dc23.pdf. [Accessed 17 Oct 2015].

[7] R. A. Grimes, "what-you-need-to-know-about-firmware-attacks," Infoworld.com, 7 Aug 2012. [Online]. Available: http://www.infoworld.com/article/2618113/security/what-you-need-to-know-about-firmware-attacks.html. [Accessed 17 Oct 2015].

[8] M. Garrett, "Securing the entire cloud with TPMs," in *Openstack Summit*, Vancouver, 2015.

ABOUT THE AUTHOR

Daksha Bhasker

MS, MBA, CISM, CISSP

Daksha Bhasker, MS, MBA, CISM, CISSP, has over a decade of experience in the telecommunications industry working in various roles from business intelligence, strategy planning, business management operations and controls, governance, SOx compliance, complex technical solutions, security risk management and cyber security. She currently works as a senior security architect focused on securing emerging technologies with the network technology development team at Bell Canada.

FREE State-of-the-Art Reports (SOARs)

The following reports are available for a limited time at no cost.

You only pay for postage ($6.00 for the first report, $2.00 for each additional).

Measuring Cyber Security and Information Assurance (2009)

This Information Assurance Technology Analysis Center (IATAC) State of the Art Report (SOAR) provides a representative overview of the current state of the art of the measurement of cyber security and information assurance (CS/IA). It summarizes the progress made in the CS/IA measurement discipline and advances in CS/IA measurement research since 2000.

Software Security Assurance (2007)

This Information Assurance Technology Analysis Center (IATAC) State-of-the-Art Report (SOAR) describes the current "state-of-the-art" in software security assurance. It provides an overview of the current state of the environment in which defense and national security software must operate than surveys current and emerging activities and organizations involved in promoting various aspects of software security assurance.

The Insider Threat to Information Systems (2008)

This publication is For Official Use Only (FOUO)

ORDERING THIS REPORT REQUIRES A .MIL OR .GOV EMAIL ADDRESS, WHICH WILL BE CONFIRMED ON PLACEMENT OF ORDER.

This Information Assurance Technology Analysis Center (IATAC) State-of-the-Art Report (SOAR) describes the current "state-of-the-art" in the understanding and awareness of, and technical and non-technical countermeasures to the insider threat to information systems. It provides an overview of the current state of the understanding in the defense, civil government, industry, and academic sectors of who "insiders" are, how they operate, what threats they pose to information systems, and what motivates them.

Security Risk Management for the Off-the-Shelf (OTS) Information and Communications Technology (ICT) Supply Chain (2010)

ORDERING THIS REPORT REQUIRES A .MIL OR .GOV EMAIL ADDRESS, WHICH WILL BE CONFIRMED ON PLACEMENT OF ORDER.

This Information Assurance Technology Analysis Center (IATAC) State of the Art Report provides a comprehensive examination of the current state-of-the-art in addressing Supply Chain Risk Management (SCRM) as it pertains to Information and Communications Technology (ICT). It provides an overview of how supply chain and SCRM are understood in government, industry, and academia.

CSIAC

AVAILABLE AT: https://www.csiac.org/store

Quantum Key Distribution: Boon or Bust?

Logan O. Mailloux
Air Force Institute of Technology

Michael R. Grimaila
Air Force Institute of Technology

Douglas D. Hodson
Air Force Institute of Technology

Colin V. McLaughlin
Naval Research Lab

Gerald B. Baumgartner
Laboratory for Telecommunication Sciences

ABSTRACT: *Quantum Key Distribution (QKD) is an emerging cybersecurity technology which exploits the laws of quantum mechanics to generate shared secret keying material between two geographically separated parties. The unique nature of QKD shows promise for high-security applications such as those found in banking, government, and military environments. However, real-world QKD systems contain a variety of implementation non-idealities which can negatively impact system security and performance. This article provides an introduction to QKD for security professionals and describes recent developments in the field. Additionally, comments are offered on QKD's advantages (i.e., the boon), its drawbacks (i.e., the bust), and its foreseeable viability as a cybersecurity technology.*

Quantum Key Distribution (QKD) is an emerging cybersecurity technology which provides the means for two geographically separated parties to grow "unconditionally secure" symmetric cryptographic keying material. Unlike traditional key distribution techniques, the security of QKD rests on the laws of quantum mechanics and not computational complexity. This unique aspect of QKD is due to the fact that any unauthorized eavesdropping on the key distribution channel necessarily introduces detectable errors (Gisin, Ribordy, Tittel, & Zbinden, 2002). This attribute makes QKD desirable for high-security environments such as banking, government, and military applications. However, QKD is a nascent technology where implementation non-idealities can negatively impact system performance and security (Mailloux, Grimaila, Hodson, Baumgartner, & McLaughlin, 2015). While the QKD community is making progress towards the viability of QKD solutions, it is clear that more work is required to quantify the impact of such non-idealities in real-world QKD systems (Scarani & Kurtsiefer, 2009).

Written for security practitioners, managers, and decision makers, this article provides an accessible introduction to QKD and describes this seemingly strange quantum communications protocol in readily understandable terms. Additionally, this article highlights recent developments in the field from the 5th international Quantum Cryptography conference (QCrypt) hosted in fall of 2015 with an eye towards the US hosted conference in 2016. Lastly, we comment on several of

QKD's advantages (i.e., the boon) and its drawbacks (i.e., the bust) while also considering QKD's viability as a cybersecurity technology.

What is QKD?

The genesis of QKD traces back to the late 1960s, when Stephen Wiesner first proposed the idea of encoding information on photons to securely transfer messages (Wiesner, 1983). In 1984, the physicist Charles Bennett and cryptographer Gilles Brassard worked together to mature this idea by introducing the first QKD protocol, known as "BB84" (Bennett & Brassard, 1984). Five years later, they built the first QKD prototype system which was said to be "secure against any eavesdropper who happened to be deaf" as it made audible noises while encoding crypto key onto single photons (Brassard, 2006). From its relatively humble beginnings, QKD has gained global interest as a unique cybersecurity solution with active research groups across North America, Europe, Australia, and Asia. Moreover, commercial offerings are now available from several vendors around the world: ID Quantique, SeQureNet, Quintessence Labs, MagiQ Technologies, Qasky Quantum Science Technology, and QuantumCTek (Oesterling, Hayford, & Friend, 2012).

Figure 1 illustrates a notional QKD system architecture consisting of a sender "Alice," a receiver "Bob," a quantum channel (an optical fiber or line-of-sight free space path), and a classical channel (a conventional network connection). Alice is shown with a laser source configured to generate single photons, while Bob measures them using specialized Single Photon Detectors (SPDs). The QKD system provides a point-to-point solution for generating shared secret key, , which can be used to encrypt sensitive data, voice, or video communications as desired by the user.

Commercial QKD systems often use the secret key to increase the security posture of traditional symmetric encryption algorithms through frequent re-keying. For example, a QKD system can be used to update a 256-bit AES key once a second. This increases the cryptosystem's security posture by significantly reducing the time and information available to an adversary for performing cryptanalysis.

Alternatively, QKD systems can be used to provide an unlimited supply of secret keying material for use in the one-time pad encryption algorithm – the only known cryptosystem to achieve perfect secrecy (Vernam, 1926), (Shannon, 1949). However, the one-time pad has strict keying requirements, which are not easy to meet with conventional technologies. More specifically, the keying material must be: 1. truly random, 2. never reused, and 3. as long as the message to be encrypted. Thus, the appeal of QKD is found in its ability to generate (or grow) shared cryptographic key, making unbreakable one-time pad encryption configurations possible.

How Does QKD Work?

To understand how QKD works, we describe the original BB84 prepare-and-measure, polarization-based protocol as it remains a popular implementation choice and is relatively easy to understand compared to other QKD protocols (Gisin, Ribordy, Tittel, & Zbinden, 2002).

Figure 2 illustrates the QKD protocol as a series of eight steps. While these steps (or processes) can be depicted in a number of ways, we have chosen this flow to clearly illustrate how the QKD protocol behaves. In an actual system, these steps would most likely overlap and/or execute in parallel. Note that *Quantum Exchange* is the only step where the laws of quantum mechanics are directly applicable.

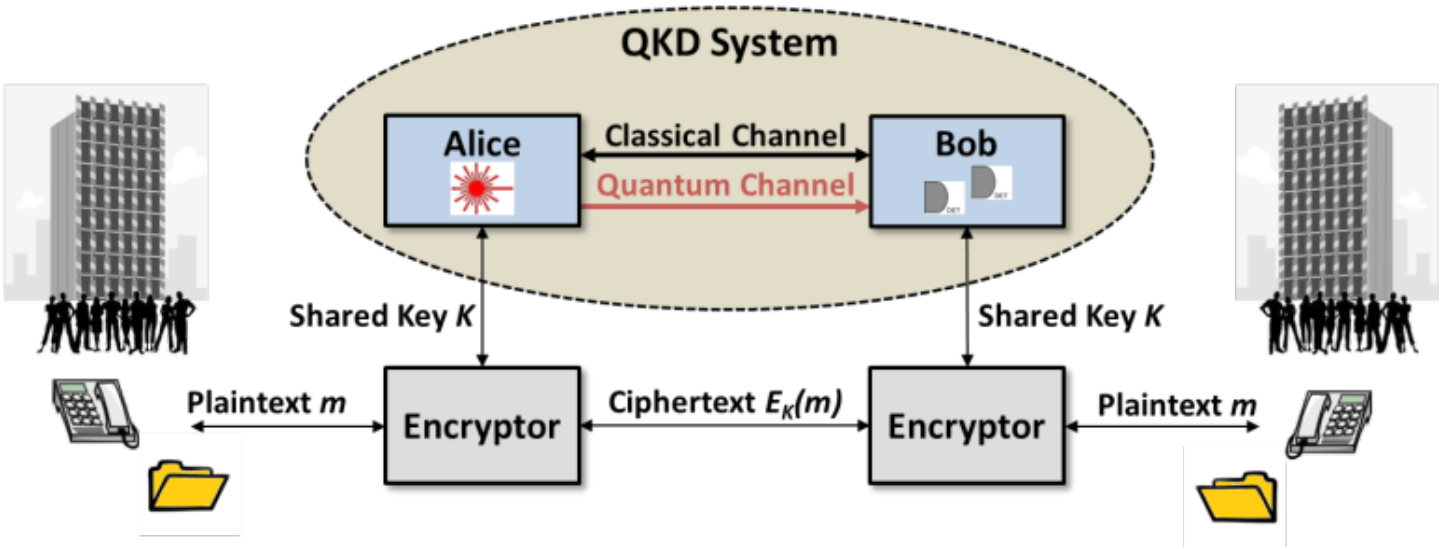


Figure. 1. Quantum Key Distribution (QKD) system context diagram. The sender "Alice" and receiver "Bob" are configured to generate shared secret key for use in bulk encryptors, where the quantum channel (i.e., a free space or optical fiber link) is used to securely transmit single photons and the classical channel is used to control specific QKD processes and protocols.

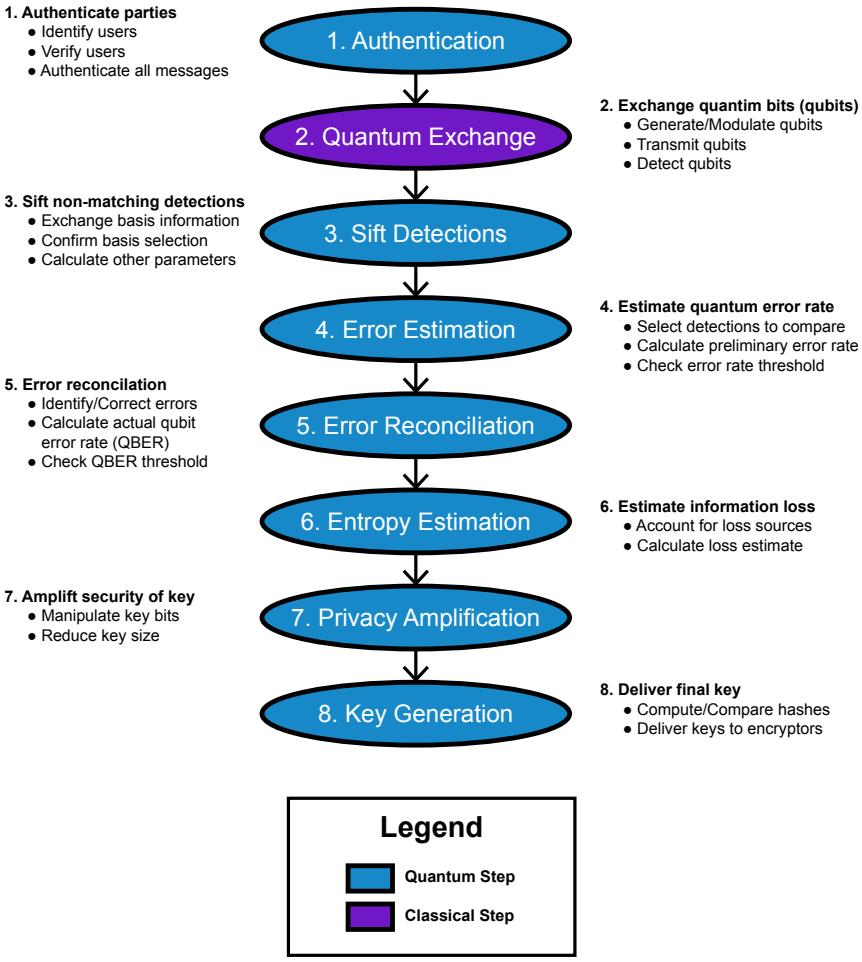


Figure. 2. Eight steps of the Quantum Key Distribution (QKD) process.

Somewhat of a misnomer, most of the QKD protocol is achieved through classical information theory "post-processing" steps.

In step 1, Alice and Bob authenticate with each other to ensure they are communicating with the expected party. Typically, this authentication is accomplished with the lesser known Wegman-Carter authentication technique to meet QKD's unconditional security claim (Scarani, et al., 2009). Moreover, unlike most cyber systems which authenticate only when initiating communications, QKD systems often utilize a transactional authentication scheme where authentication occurs after each step (or a sequence of steps) according to the specific system implementation.

Table 1. The prepare and measure, polarization-based BB84 QKD protocol.

Alice prepares single photons			Bob measures single photons	
Random encoding basis	Random bit value	Prepared photon state	Random decoding basis	Measurement result
⊕	0	$\|\leftrightarrow\rangle$	⊕	0 or 1
⊕	1	$\|\updownarrow\rangle$	⊗	Random
⊗	0	$\|\swarrow\rangle$	⊕	Random
⊗	1	$\|\searrow\rangle$	⊗	0 or 1

During quantum exchange (step 2), Alice prepares single photons, known as quantum bits or "qubits," in one of four polarization states $|\leftrightarrow\rangle$, $|\updownarrow\rangle$, $|\swarrow\rangle$, or $|\searrow\rangle$. The photon's polarization state is prepared according to a randomly selected basis and bit value as shown in Table 1. Each photon is then transmitted to Bob through the quantum channel, where it can be subject to significant loss (e.g., >90% loss is common). This is due to the loss that is experienced by single photons when they propagate over long distances through optical fiber or line-of-sight free space links. Due to the inherent challenges of single photon propagation, a majority of Alice's photons are lost during transmission, thereby limiting the system's effective operational distance to <100 km (Scarani, et al., 2009).

Assuming Alice's encoded photon arrives at Bob, he must randomly select a measurement basis for each detected photon. If Bob measures the photon with the correctly matching basis, the encoded bit value (0 or 1) is obtained with a high degree of confidence. Conversely, if Bob measures the photon with the incorrect basis, a random result occurs and the originally prepared bit value is destroyed. This quantum mechanical phenomenon underpins QKD's secure key generation where measuring a photon in flight forces its encoded state to collapse and prevents accurate copies from being made (i.e., the No Cloning Theorem) (Wootters & Zurek, 1982). Quantum exchange results in a series

of detections at Bob, which need to be correlated with Alice's sent photons through a sifting process.

In step 3, Bob's detections are sifted to eliminate incorrect (non-matching) basis measurements. In general, 50% of Bob's detections will be in the wrong basis and sifted out because of his random basis selection. This results in a shared sifted key, known as the "raw key," in both Alice and Bob approximately half the size of Bob's initial set of detections.

Next, an estimate of the quantum exchange error rate is calculated in step 4. Typically, a random percentage of bits are selected and compared over the classical channel. The estimated error rate is used to inform the error reconciliation technique (step 5), and can also be used to conduct an initial security check. This step is particularly important for QKD's theoretical security posture as all errors during quantum exchange are attributed to eavesdroppers since the QKD protocol cannot discriminate between noise and malicious interference. Thus, if the estimated error rate exceeds the predetermined QKD error threshold (e.g., 11%), the raw key must be discarded as an adversary is assumed to be listening (Scarani, et al., 2009). Typically, the key generation is then restarted.

In step 5, error reconciliation is performed to correct any errors in Alice and Bob's raw keys. Due to device non-idealities and physical disturbances during quantum exchange, expected error rates are typically 3-5% (Gisin, Ribordy, Tittel, & Zbinden, 2002). Error reconciliation techniques employ specialize bi-directional correction algorithms (e.g., Winnow, Cascade, or Low-Density Parity-Check) to minimize the amount of information "leaked" over the classical channel to eavesdroppers (Scarani, et al., 2009). With a high probability, this step results in a perfectly matched, error free shared secret key between Alice and Bob. The error reconciliation step results in a formalized Quantum Bit Error Rate (QBER), which is again checked against the QKD security proof threshold (e.g., 11%) to determine if an eavesdropper is listening on the quantum key distribution channel (Scarani, et al., 2009). If the security threshold is exceeded, the key must be discarded and the process is restarted.

Next, entropy estimation (step 6) accounts for the amount of secret key information leaked while executing the QKD protocol steps. For example, during quantum exchange, information leakage occurs from non-ideal laser sources which produce insecure multi-photon pulses. In another example, error reconciliation communications over the classical channel leaks information about the secret key. In general, conservative loss estimates are made; however, implementations may differ considerably (Slutsky, Rao, Sun, Tancevski, & Fainman, 1998). The entropy estimate is then passed to the privacy amplification step, which corrects for the information leakage and ensures the eavesdropper has negligible information regarding the QKD-generated shared secret key. More specifically, step 7 employs advanced information theory techniques such as a universal hash function to produce a more secure final shared secret key (Scarani, et al., 2009).

Lastly, in order to ensure the final symmetric crypto keys are the same, a hash of Alice and Bob's keys are compared. If they match, the keys are delivered to the system owner. These unconditionally secure shared symmetric keys can then be used as desired by the user to protect sensitive information with the unbreakable one-time pad encryption scheme or supplement more practical encryption schemes such as AES. For readers interested in more details, a security-oriented description of QKD is available in (Mailloux, Grimaila, Hodson, Baumgartner, & McLaughlin, 2015) with comprehensive physics based discussions in (Scarani, et al., 2009) and (Gisin, Ribordy, Tittel, & Zbinden, 2002).

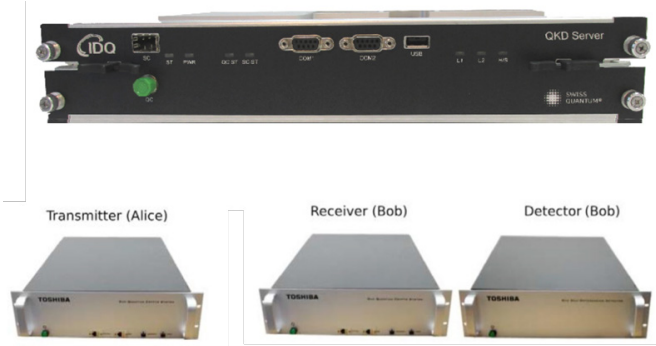


Figure 3. The ID Quantique (IDQ) rack mountable QKD system is shown on the top (ID Quantique, 2016) and the Toshiba record holding hybrid QKD system is shown on the bottom (Dixon, et al., 2015).

Observations from Quantum Cryptography Conference (QCrypt) 2015

Over the past several years, the annual QCrypt conference has served as the world's premier forum for students and researchers to present and collaborate on all aspects of quantum cryptography. QCrypt is also the primary forum for announcing the year's best QKD results. In late 2015, the fifth QCrypt conference was hosted in Tokyo, Japan and attended by more than 275 participants with a largely international audience of physicists, information theorists, and cryptographers (Quantum Cryptography Conference, 2016). From this conference, key observations are offered for the reader to gain perspective on recent developments in the quantum cryptography field.

- **Striving for Commercial Viability** – QCrypt 2105 began with several demonstrations and talks focused on practically-oriented QKD systems which balance cost, performance, and security trades towards affordability. In particular, the QKD industry leader, ID Quantique, unveiled a completely redesigned QKD blade system which employs a new quantum exchange protocol, anti-tamper precautions, and additional security features to mitigate quantum attacks (ID Quantique, 2016). Likewise, Toshiba Research Laboratory Europe, supported by Japan's National Institute of Information and Communications Technology, prominently displayed their record breaking QKD system. The Toshiba system boasts the world's highest key rates, improved user interface, and automated synchronization for increased usability over metropolitan distances (Dixon, et al., 2015). Unlike early experimental QKD configurations, these systems are designed to be rack mountable and more

easily integratable into existing communications structures. Figure 3 shows both the commercially viable ID Quantique and Toshiba QKD systems.

- **Fielding QKD Networks –** For distributed networks and long distance operation, QKD requires the use of either quantum repeaters or satellite-based solutions. While fully functional quantum repeaters are years away from being realized, simpler stop-gap "trusted node" configurations have been successfully fielded (Scarani, et al., 2009). These QKD networks utilize a series of back-to-back QKD systems to cover larger metropolitan areas and support long-haul backbone distances. Using this method, China is building the world's largest QKD network along its west coast employing 46 nodes to cover some 2,000 km (Wang, et al., 2014). Similarly, one of the conference's keynotes, the US research organization Battelle, described their development of trusted nodes with ID Quantique to support a 1,000 km planned run from Columbus, Ohio to Washington, D.C. (Quantum Cryptography Conference, 2016). With respect to satellite-to-ground QKD, research centers in America, Canada, Europe, Japan, and China are exploring the feasibility of and conducting experiments to prove the feasibility of transmitting single photons from a Low Earth Orbit (LEO) satellite through the Earth's turbulent atmosphere. Most notably, China is actively pursuing their goal of launching a QKD satellite by 2016 (Bieve, 2016). Figure 4 depicts both China's terrestrial QKD network and their planned space-based QKD links.
- **Barriers to Acceptance –** While a majority of the research-focused conference is focused on improvements to QKD protocols, quantum hardware, and information theory advancements, arguably, the most important theme of the conference pertained to the acceptance of QKD (or lack thereof) as a cybersecurity solution. As repeatedly recognized during QCrypt 2015, several significant barriers to QKD's acceptance exist. This was perhaps best captured by the field's most recognized researcher, Dr. Nicolas Gisin, who boldly stated "The quantum technology era has started… In 10 years either QKD will have found its markets or will be dead" (Gisin, 2015). In a cybersecurity community that typically adopts new technological solutions rather quickly, quantum based security technologies are slow to be adopted. Perhaps, security professionals are uncomfortable with the topic of quantum mechanics? Or perhaps, QKD developers are just now starting to make progress on critical implementation security issues, interoperability standards, and formal certifications (ETSI, 2015).

From these overarching conference themes, we next elaborate on some of QKD's advantages and disadvantages in order to help security professionals better understand the technology and its application. Thus, while a bit subjective in nature, and not without debate, we've chosen to describe three ways in which QKD is a boon to the cybersecurity community and three ways in which it is a bust.

The Boon

While there are several ways to describe the advantages of QKD, in this article the authors' have chosen to approach this challenge from the user's perspective. Meaning, we desire to provide a useful commentary which addresses the utility of QKD (and its related developments) for an end user and not merely elaborate on the merits of its research or what it could be.

1. **Generates Unconditionally Secure Keying Material –** Leveraging the laws of quantum mechanics, QKD is the only known means which can grow unlimited amounts of symmetric keying material to effectively employ the one-time pad cryptosystem (the only unbreakable encryption scheme known). This formalized information-theoretic security foundation is much stronger than conventional encryption techniques which depend on demonstrated computational complexity. This is precisely why QKD has gained global recognition as an emerging cybersecurity technology in the face of quantum computing advances which threaten other conventional cryptosystems such as RSA.
2. **Quantum Random Number Generators –** In order to maintain their information-theoretic security posture, QKD systems require true sources of randomness. Thus, the advancement of QKD has successfully facilitated the development of quantum random number generators. These devices provide a physical source of randomness based on quantum phenomenon which is desirable for cryptographic devices, software applications, and other industries. Of note, the gaming/gambling industry is said to be the world's largest consumer of random number generators and a fiscally rewarding enterprise. While QKD upstarts seem to come and go, there is a definite need for cheap and reliable sources of entropy in the commercial market.
3. **Strengthens the Cybersecurity Field –** QKD encourages multidisciplinary collaboration amongst information theorists, engineers, cryptography experts, security professionals, and physicists that may not occur otherwise. Establishing these types of interactions is critical for advancements in several cyber related fields such as quantum communication, quantum sensing, and quantum computing. For example, the integration of computer scientists and quantum physicists is necessary for the development and utilization of quantum computing algorithms. On a related note, QKD has also brought about the occurrence of "Quantum Hacking" (Institute of Quantum Computing, University of Waterloo, 2014). This growing specialty area is testing the security of new quantum technologies and protocols, and perhaps someday, we'll even have security assessments which include quantum red teams.

The Bust

QKD systems have performance limitations, device non-idealities, and system vulnerabilities which are not well understood (Scarani & Kurtsiefer, 2009). Thus, potential users often question both the effectiveness of the technology and its system security posture. For QKD to be accepted as a cybersecurity technology the following critical issues (at a minimum) should be addressed.

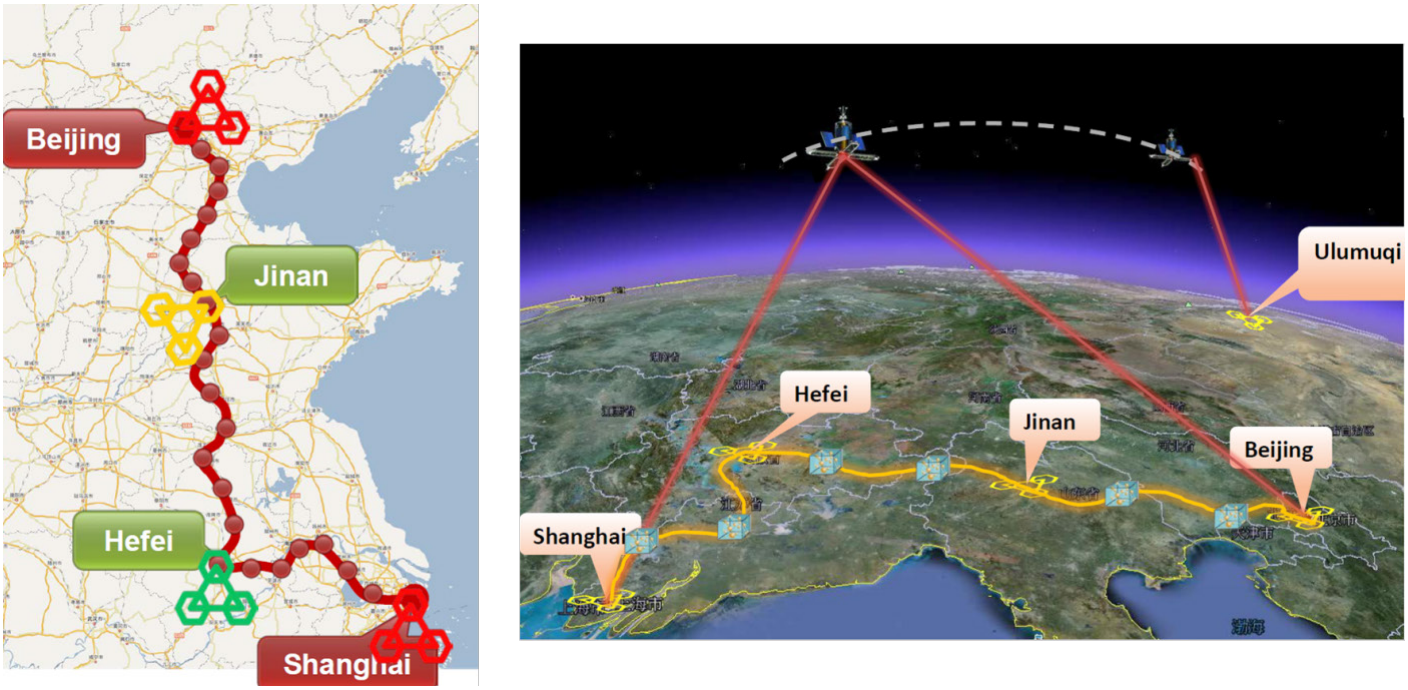


Figure 4. China's 46 node terrestrial QKD network is shown on the left and the planned space-based QKD network is shown on the right (Quantum Cryptography Conference, 2016).

1. **QKD is Point-to-Point Technology –** Because QKD is a point-to-point solution, it does not scale well for modern communications infrastructures. While gains are being made towards networked key management solutions, they are fundamentally limited by QKD's quantum underpinnings, which prevent the amplification of single photons (Wootters & Zurek, 1982). Given this critical limitation, QKD does not appear to be a good fit for wide scale implementation and may only be viable for specialized two site applications such as encrypted voice communications in a metropolitan area.
2. **Implementation Security Vulnerabilities –** QKD systems have implementation non-idealities which introduce vulnerabilities and negatively impact both performance and security. For example, these "unconditionally secure" QKD systems protocols are vulnerable to attacks over the quantum channel, including man-in-the-middle (authentication failures), intercept/resend (measuring and replacing photons), photon number splitting (stealing photons), and blinding optical receivers (unauthorized laser sources). Additionally, QKD systems are also vulnerable to common cybersecurity attacks against computers, applications, and protocols. These implementation security issues and their resulting vulnerabilities must be well-studied and addressed through established architectural design principles, verifiable designs, and assured operational configurations to provide trustworthy systems to end users.
3. **No Formal Certification Method –** As high-security crypto devices, QKD systems should undergo formal security assessments and certification processes to address (at a minimum) physical attacks, side channel analysis, and data manipulation. However, within the QKD community there is little discussion thereof, and arguably sluggish progress towards an independent certification process (ETSI, 2015). Furthermore, QKD developers must adopt a more holistic view of security including proactive techniques such as assuring secure operational baselines and continuous monitoring of the system's communication links.

Despite QKD's drawbacks, the technology does show promise as an enabler to unbreakable encryption (i.e., generating unlimited amounts of random key for use in On-Time Pad encryption) for niche applications such as point-to-point communications and data transfer.

Conclusion

Security professionals recognize that ongoing advancements in quantum computing (along with Shor's algorithm for quickly factoring large prime numbers) threaten the security of modern public key cryptography techniques such as RSA (Monz, et al., 2015). Thus, new *post-quantum* security solutions need to be given serious consideration as indicated by the National Security Agency's recent announcement specifying "a transition to quantum resistant algorithms" for their cryptographic Suite B algorithms (NSA, 2015). While this transition will occur slowly over time, organizations with significant data protection requirements such as the US Government (i.e., 25 years of data protection) must start thinking about post-quantum crypto solutions now.

While unbreakable one-time pad encryption solutions enabled by QKD provide the ultimate protection available (they are proven secure against advances in quantum computing), they do not fit well into the established communications infrastructure. Conversely, quantum resistant algorithms (encryption techniques which are shown to not be easily broken by quantum computers) have the benefit of fitting nicely into the existing infrastructure (Bernstein, 2009).

With an eye towards QCrypt 2016, hosted by the US based Joint Center for Quantum Information and Computer Science, perhaps the QKD community will begin to adopt a wider perspective on the field of quantum cryptography. For example, the US's premier quantum center seeks to more broadly advance the state of the art in quantum algorithms, quantum communication, and quantum computing instead of merely focusing on QKD (University of Maryland, 2016). Moreover, the US National Institute of Standards and Technology (NIST) recently stood up a multi-year project to explore quantum resistant algorithms (2016) and a new international conference series on post-quantum cryptography is quickly gaining attention (2016). Perhaps, these events are evidences that a change is occurring in the QKD community, an evolution towards more viable cryptographic solutions. ■

Acknowledgments

This work was supported by the Laboratory for Telecommunication Sciences [grant number 5743400-304-6448].

Disclaimer

The views expressed in this paper are those of the authors and do not reflect the official policy or position of the United States Air Force, the Department of Defense, or the U.S. Government.

BIBLIOGRAPHY

[1] Bennett, C. H., & Brassard, G. (1984). Quantum cryptography: public key distribution and coin tossing. *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, *175, no. 0.*

[2] Bernstein, D. J. (2009). *Post-quantum cryptography.* Springer.

[3] Bieve, C. (2016, January 13). *China's quantum space pioneer: We need to explore the unknown*. Retrieved from Nature: http://www.nature.com/news/china-s-quantum-space-pioneer-we-need-to-explore-the-unknown-1.19166

[4] Dixon, A. R., Dynes, J. F., Lucamarini, M., Fröhlich, B., Sharpe, A. W., Plews, A., . . . al., e. (2015). High speed prototype quantum key distribution system and long term field trial. *Optics Express, 23*(6), 7583-7592.

[5] ETSI. (2015, June 08). *Quantum key distribution standards*. Retrieved from www.etsi.org/technologies-clusters/technologies/quantum-key-distribution

[6] Gisin, N. (2015, October 21). *Quantum Cryptography: where do we stand?* Retrieved from https://www.youtube.com/watch?v=Vk9T-tVAI4c&feature=youtu.be

[7] Gisin, N., Ribordy, G., Tittel, W., & Zbinden, H. (2002). Quantum cryptography. *Reviews of Modern Physics, 74*(1), 145-195. Retrieved from 10.1103/RevModPhys.74.145

[8] ID Quantique. (2016). Retrieved from http://www.idquantique.com/

[9] Institute of Quantum Computing, University of Waterloo. (2014). *Quantum hacking lab*. Retrieved Mar 14, 2014, from http://www.vad1.com/lab/

[10] Mailloux, L. O., Grimaila, M. R., Hodson, D. D., Baumgartner, G., & McLaughlin, C. (2015). Performance evaluations of quantum key distribution system architectures. *IEEE Security and Privacy, 13*(1), 30-40.

[11] *Science, 351*(6277), 1068-1070. Monz, T., Nigg, D., Martinez, E. A., Brandl, M. F., Schindler, P., Rines, R., . . . Blatt, R. (2015). Realization of a scalable Shor algorithm.

[12] NIST. (2016, March 07). *Post-Quantum Crypto Project*. Retrieved April 09, 2016, from http://csrc.nist.gov/groups/ST/post-quantum-crypto/

[13] NSA. (2015, August 19). *Cryptography Today*. Retrieved from Information Assurance: https://www.nsa.gov/ia/programs/suiteb_cryptography/

[14] Oesterling, L., Hayford, D., & Friend, G. (2012). Comparison of commercial and next generation quantum key distribution: Technologies for secure communication of information. *Homeland Security (HST), 2012 IEEE Conference on Technologies for*, (pp. 156-161). Retrieved from http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6459842

[15] Post-Quantum Cryptography. (2016, January 18). *Post-Quantum Crypto 2016*. Retrieved January 18, 2016, from https://pqcrypto2016.jp/

[16] Quantum Cryptography Conference. (2016). *QCrypt 2015*. Retrieved from 2015.qcrypt.net

[17] Scarani, V., & Kurtsiefer, C. (2009). The black paper of quantum cryptography: real implementation problems. *Theoretical Computer Science, 560(1), 27–32.*

[18] Scarani, V., Bechmann-Pasquinucci, H., Cerf, N. J., Dušek, M., Lütkenhaus, N., & Peev, M. (2009). The security of practical quantum key distribution. *Reviews of Modern Physics, 81*(3), 1301-1350. Retrieved from ttp://dx.doi.org/10.1103/RevModPhys.81.1301

[19] Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell System Technical Journal, 28*, 656-715.

[20] Slutsky, B., Rao, R., Sun, P.-C., Tancevski, L., & Fainman, S. (1998). Defense frontier analysis of quantum cryptographic systems. *Applied Optics, 37*(14), 2869-2878.

[21] University of Maryland. (2016, April 30). *Joint Center for Quantum Information and Computer Science*. Retrieved from http://quics.umd.edu/

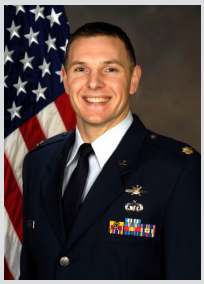
[22] Vernam, G. S. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *American Institute of Electrical Engineers, Transactions of the, 45*, 295-301.

[23] Wang, S., Chen, W., Yin, Z.-Q., Li, H.-W., He, D.-Y., Li, Y.-H., . . . et al. (2014). Field and long-term demonstration of a wide area quantum key distribution network. *Optics Express, 22*(18), 21739-21756.

[24] Wiesner, S. (1983). Conjugate coding. *ACM Sigact News, 15*(1), pp. 78-88. Retrieved from http://dx.doi.org/10.1145/1008908.1008920

[25] Wootters, W. K., & Zurek, W. H. (1982). A single quantum cannot be cloned. *Nature,* 299(5886), 802-803. doi:10.1038/299802a0

ABOUT THE AUTHORS



Logan O. Mailloux
Air Force Institute of Technology

Logan O Mailloux, CISSP, CSEP (BS 2002, MS 2008, PhD 2015) is a commissioned officer in the United States Air Force and Assistant Professor at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. His research interests include system security engineering, complex information communication and technology implementations, and quantum key distribution systems. He is a member of Tau Beta Pi, Eta Kappa Nu, INCOSE, the ACM, and IEEE.

Douglas D. Hodson
Air Force Institute of Technology

Douglas D Hodson (BS 1985, MS 1987, PhD 2009) is an Assistant Professor of Software Engineering at the AFIT, Wright-Patterson AFB, Ohio, USA. His research interests include computer engineering, software engineering, real-time distributed simulation, and quantum communications. He is also a DAGSI scholar and a member of Tau Beta Pi.

Michael R. Grimaila
Air Force Institute of Technology

Michael R Grimaila, CISM, CISSP (BS 1993, MS 1995, PhD 1999, Texas A&M University) is Professor and Head of the Systems Engineering department and member of the Center for Cyberspace Research (CCR) at the Air Force Institute of Technology (AFIT), Wright-Patterson AFB, Ohio, USA. He is a member of Tau Beta Pi, Eta Kappa Nu, the ACM, a Senior Member of the IEEE, and a Fellow of the ISSA. His research interests include computer engineering, mission assurance, quantum communications and cryptography, data analytics, network management and security, and systems engineering.

Colin V. McLaughlin
Naval Research Lab

Colin V McLaughlin, PhD (BA 2003, PhD 2010) is a Research Physicist at the United States Naval Research Laboratory, Washington, D.C., USA. He specializes in photonic communication devices and systems.

Gerald B. Baumgartner
Laboratory for Telecommunication Sciences

Gerald B. Baumgartner, PhD (BS 1971, MS 1973, PhD 1980, Illinois Institute of Technology) is a Research Physicist at the Laboratory for Telecommunications Sciences, College Park, Maryland, USA. He is a member of the American Physical Society, the Optical Society of America and the Society for Industrial and Applied Mathematics. Dr Baumgartner's research interests include quantum optics, quantum communications, quantum information, communications security, communications system modeling and simulation and statistical signal processing.

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 the Journal.

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.

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, 300 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

Michael Weir, CSIAC Director
John Dingman, Managing Editor
Email: info@csiac.org

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 THE JOURNAL OF CYBER SECURITY AND INFORMATION SYSTEMS

COVER DESIGN

SHELLEY HOWARD
Graphic Designer
Quanterion Solutions

Distribution Statement
Unclassified and Unlimited

CSIAC
100 Seymour Road
Utica, NY 13502-1348
Phone: 800-214-7921 • **Fax:** 315-732-3261
E-mail: info@csiac.org
URL: https://www.csiac.org/

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.

CORRECTIONS FROM VOLUME 4, ISSUE 1:

COVER ILLUSTRATION

Keri Burkhart, AFRL

PAGES 45 AND 46

Photos in article titled "The Junior Force Council: Reaching Out to New Employees"
Al Santacroce, AFRL

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.4, No 2"

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: 315-732-3261
E-mail: info@csiac.org

An archive of past newsletters is available at **https://journal.csiac.org**.

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 – June 2016

— IN THIS ISSUE —