National Cybersecurity Institute Journal

Volume 1, No.2

National Cybersecurity Institute Journal

Volume 1, No. 2

5. Is There a Cyber War? Review Essay
Matthew J. Flynn, PhD

9. Cyber Warfare Simulation to Prepare to Control Cyber Space
Martin R. Stytz, PhD
Sheila B. Banks, PhD

26. Multidisciplinary Approaches for Cyber Security
J. Todd McDonald, PhD
Lee M. Hively, PhD

33. Geospatial Mapping of Internet Protocol Addresses for Real-Time Cyber Domain Visual Analytics and Knowledge Management Using the Global Information Network Architecture
Thomas Anderson, PhD
Curtis L. Blais
Don Brutzman
Scott A. McKenzie

51. The New Demands of Online Reputation Management
Shannon M. Wilkinson
Editing and Research by Christopher Hampton

57. The Risk of Cyber Crimes to the Critical National Infrastructure: A Threat Assessment
Brian A. Lozada

64. Making the Community Project Approach Work in Your Community
Denise M. Pheils, PhD

 | ISSN 2333-7184

NATIONAL CYBERSECURITY INSTITUTE JOURNAL

The National Cybersecurity Institute at Excelsior College is a research center based in Washington, DC, dedicated to increasing knowledge of the cybersecurity discipline and its workforce demands. Published three times a year, the peer-reviewed *National Cybersecurity Institute Journal* covers topics that appeal to a broad readership within the cybersecurity discipline, with a particular focus on education, training, and workforce development. The manuscripts submitted to the journal are reviewed for their contribution to the advancement of applied research in the area of cybersecurity.

Submission guidelines for authors can be found at www.nationalcybersecurityinstitute.org/journal/.

FROM THE EDITOR

Welcome to Volume 2 of the *National Cybersecurity Institute Journal* (NCIJ). Since our last issue there has been a good deal of news related to cybersecurity with many notable cyber breaches. As always, the mission of NCI and our journal is to increase awareness and knowledge of the cybersecurity discipline to help others better understand and meet the escalating challenges in the cyber community. In this latest issue, you will find seven informative articles from notable authors with a variety of perspectives on the field.

In the first article, Dr. Matthew Flynn, a professor at the Marine Corps University, offers a review of recent essays in his offering "Is There a Cyber War?" Professors Martin Stytz and Sheila Banks propose using a data/situational awareness-based orientation for assessing tactical and strategic cyber offensive and defensive activities in their article. Dr. J. Todd McDonald and Dr. Lee Hively provide us with food for thought as they argue that holistic and collaborative efforts foster the best environment for advancing the field of cybersecurity. Thomas Anderson, Curtis Blais, Don Brutzman, and Scott McKenzie discuss the use of GINA to create a System of Systems in the cyber domain specifically to read and process data from the MMOWGLI bii game into a GIS analysis tool in near real-time. Shannon M. Wilkinson, working in collaboration with Christopher Hampton, discusses the evolving issue of protecting your reputation with their offering titled "The New Demands of Online Reputation Management." Brian Lozada provides us with an article about cyber crime with his piece titled "The Risk of Cyber Crimes to the Critical National Infrastructure: A Threat Assessment." And in our last article, Dr. Denise Pheils provides an interesting perspective to obtaining work experience in her article "Making the Community Project Approach Work in Your Community."

We believe that these articles should educate our readers and provide them with information that they can apply to their own systems and organizations.

The security of a digital system is of great importance, and we work diligently to obtain and publish articles that our readers will find useful. A great many thanks go to all the contributors, administration, and staff for their efforts to bring this latest edition of the *National Cybersecurity Institute Journal* to our readers. I look forward to your comments, suggestions, and future submissions to the journal.

Dr. Jane A. LeClair
Editor in Chief

Is There a Cyber War? *Review Essay*

Matthew J. Flynn, PhD

When it comes to seeking a better understanding of whether there is a war in cyberspace or not, one refers to the studies and reports of think tanks and the limited number of scholarly books published on the topic. Two main extreme points of view stand out in this kind of research: on the one hand, Richard Clarke and Robert K. Knake's, *Cyber War: The Next Threat to National Security and What to Do About It* (2010), offers a dire prediction of a looming conflict, and on the other hand, Thomas Rid's, *Cyber War Will Not Take Place* (2013), tries to calm the waters assuring us that cyber war is not as compelling a threat as some doomsayers claim it to be.

Think tanks like the RAND Corporation made a case that there was cyber war as early as 1993. In the wake of the First Gulf War in 1991, John Arquilla and David Ronfeldt, in a short study and a subsequent book chapter titled, "Cyberwar is Coming!" (1993), announced that the key to victory in war was information. An "information revolution" spoke to Western ascendancy during the just concluded war against Iraq, an advantage extending into the future. The rise of "netwar" where conflict ranged across all of society, as the authors characterized this new phenomena, struck an optimistic beat even as they ominously predicted war to be, well, "society-wide." The post-Cold War world had ushered in some kind of benign "total war"; a label normally associated with the disasters of war, but now associated with a competition of ideas played out bloodlessly in the recesses of cyberspace.

The years after 1991 held much promise for the United States given the military success of the American-led coalition in Iraq and the demise of the USSR. The United States had won the Cold War and with that success earned a chance to shape the world and for the better, or so it appeared. The post-9/11 world shattered much of this optimism. Either an opportunity had been missed or things had taken a turn that caught western powers, certainly the United States, by surprise. In consequence, war society-wide had not become more benign. Yet, Arquilla, now chairman of the defense analysis program at the Naval Post Graduate School, stands by his predictions today and with merit. Cyber, he argues in "Cyberwar Is Already Upon Us," a short piece in *Foreign Policy Magazine* published in February 2012, has cemented the need to think in terms of the impact of information on the battlefield and the ideological impact of that struggle. Moreover, given the rise of social media, authoritarian regimes can no longer boast of a "moral superiority" that goes unquestioned within state borders. Cyber connectivity has empowered society as a whole and hence established the concept of cyber conflicts that brought on chances for change with reduced bloodshed.

SO DOES CYBER THEN CONSTITUTE A WAR?

In *Cyberdeterrence and Cyberwar* (2009), RAND discounts such thinking in an analysis conducted by Martin Libicki. Libicki (2009) argues that cyber war does not exist onto itself, but rather functions as a tool extending confrontation into the new cyber domain. Cyber is as incapable of dictating a struggle as strategic airpower. Consequently, those attacking via cyberspace represent a "great annoyance," Libicki claims. He gives no hint that cyber war could be more devastating; this line of thinking puts Libicki in line with Arquilla. No, the most important aspect of cyber security is not overreacting to a loss of deterrence, something that is difficult to achieve in cyberspace but, again, given cyber's marginal implications in terms of military function, this failure is not on the scale of such a lapse in the

context of nuclear war. While this is a facile comparison, Libicki's effort at perspective is on the mark, a need to carefully weigh concepts such as deterrence before rendering judgment.

Throwing cold water on the idea of a standalone war in cyberspace as Libicki (2009) does in the RAND study is not a surprise because he had delivered a similar conclusion just a few years earlier in his book *Conquest in Cyber Space: National Security and Information (*2007). Conquest is not looming in cyberspace, concludes Libicki, thus leaving assessments of how this space impacts the physical world as the most important measure of any cyber war. Information is a key part of warfare, but no more than that. The idea of a contest of wills hanging on the ideological import of that information is minimized because cyber-based conquest is so difficult to achieve if, in fact, it is possible at all. In a curious loop, Libicki allows for a growing symbiotic relationship among friends, neutrals, and even adversaries in cyberspace, but he sees no shaping of enemies via this medium and only encourages a greater awareness of vulnerability in the cyber world as tied to the physical.

A number of think tanks follow suit; among these is The Center for Strategic and International Studies (CSIC) in Washington, DC. Senior Fellow James A. Lewis in *Conflict and Negotiation in Cyber Space*, released in February 2013, says that there is no cyber war, at least in standalone terms. Rather, cyber merely augments existing war. The new technology does in fact have the potential to reshuffle things along this line and it is essential to get the thinking right to keep such disturbance to a minimum. Most importantly, however, Lewis says one must realize that cyber weapons are "not decisive" and they "cannot win a conflict."

So, cyber does not get to claim a new domain or a separate conflict from the rest. Rather, it is necessary to ensure cyber threats are addressed by the international community and, therefore, tamed. In sum, with cyber, nothing has changed or has to change.

Academics are just as inclined as those in think tanks to discount the idea of a war in the cyber world. Rid's *Cyber War Will Not Take Place* (2013) suggests that the label "war" to the cyberspace domain does not fit because of the lack of violence in the domain. According to Rid (2013), war must be violent, purposeful, political, and ultimately people have to die. None of this is happening in cyberspace.

Rid's (2013) main objective is quieting voices from within military channels who are sounding the alarm of a new conflict. The discomfort of military leadership is no more than a ploy to justify a larger role in cyberspace as well as the validity of pandering for funding. So Rid (2013) would relegate those warning of a "cyber Pearl Harbor" to the back of the room; to doomsayers who have nothing to offer but fear and paranoia.

Rid has the backing of Carl Von Clausewitz, the dean of western military theory, who, in his famous tome, *On War* (1848) argued that violence had to accompany war. This narrow Clausewitzian approach highlights the extent to which think tanks and academics both discourage the theory of war in cyberspace.

While their point of view is more practical than academic, Clarke and Knake's call to arms is not so easily dismissed as one might think. In effect, they argue in *Cyber War* (2010) that the Western way of life, based on an open and transparent society and government, has created vulnerabilities in cyberspace. So any evaluation of the internet technology also assesses the value of increased connectivity as a public good. Clarke and Knake (2010) are not primarily warning of an impending doom, but they are portraying cyber war as a Western failure, an outgrowth of a system betraying itself. This is too categorical a forecast, ignoring the virtue of technology making connectivity a global reality and, therefore, a Western triumph not a liability.

In short, cyber attacks can threaten "our way of life" or deliver on this promise. This duality brings us back to Arquilla's imperative: that cyber war is coming. However, this imperative is lost in the shadow of Clausewitz. To suspend analysis of a cyber war because of the lack of violence, or greatly restrict an understanding of cyberspace because it poses no threat on its own, means giving up on the ideological premise housed in information warfare.

Netwar can in fact impact entire societies due to the connectivity caused by cyberspace. The United States possesses that weapon as cyberspace has allowed the U. S.—and really the West—to contemplate warfare that rests on an ideological advantage in cyberspace that could not be ignored by adversaries. It is important to realize that there is not just a war in cyberspace, but a Western way of war promising victory. The time has come to seize this opportunity.

Some other books talk about a more complex picture of war in cyberspace, but shrink from such a conclusion. Jeffrey Carr's book *Inside Cyber War* (2010) argues that cyber represents fighting without fighting. Here is some recognition of cyber as a unique battle space. Carr (2010) does not succumb to the idea that cyber is entirely new and must embrace new nomenclatures and measures. Rather, some familiar guidelines direct Carr's (2010) analysis such as placing cyber in the confines of international law. Moreover, his remedy hangs on "active defense," a way of again enforcing norms that resonate internationally because of the difficulty of assigning attribution to that attack. Yet, Carr's (2010) book is more of a warning of a cyber war than it is an analysis that increases understanding of such a war, an approach much like Clarke and Knake's (2010) effort. Carr tries to understand the bigger picture of cyber and that understanding requires a number of key aspects to be grouped together. Carr references six steps to define a cyber attack and a series of defense readiness conditions and scenarios for responding to cyber attacks. There is a quality of "what if" about Carr's book that plagues its analysis. As a result, Carr (2010) is still a long way from Arquilla and Ronfeldt's point, initiated in 1993, that an ideological struggle is afoot in cyberspace, and that struggle is weighted in favor of the West. Although Carr (2010) calls attention to information warfare and to the value Russia and China place on this mode of warfare, he fails to draw any conclusions.

Peter Singer and Alan Friedman draw at least one big conclusion in their book *Cybersecurity and Cyberwar: What Everyone Needs to Know* (2013). The authors state that cyber is an opportunity; for although there are still many unknowns to be revealed in the cyber world, there is no reason to be afraid. To come to this conclusion, a tour of all things cyber unfolds, much like Carr did four years earlier. The methodology is almost anecdotal as Singer and Friedman (2013) update threats, changes, and advances, and do so as they say, as two men in their thirties, witnessing the creation of cyber and anxiously awaiting its maturity. This is a hopeful message, but what might be cyber war is lost in the need for cyber security, hence casting doubt on how this vision of the goodness of cyber will come to pass.

A look at the conversation regarding the nature of cyber war reveals that an emphasis on the ideological premise deep-rooted in the medium is missing. This is a key point of analysis because the issue of all things cyber being good, or the internet of things being an exaggeration and far short of a necessity, hangs in the balance. Yet, the discussion of the cultural ramifications of connectivity via the Internet merits close scrutiny and endorsement far beyond a measure of convenience for civilian consumption. The war that is unfolding here is an ideological one presenting the United States with a great advantage. A new form of military engagement is at hand in cyberspace, one that is dominated by civilians, and one that hopefully is improving security in that domain without encroaching on freedoms, hence defining cyberspace as a Western way of life and a virtue.

REFERENCES CITED

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming!. *Comparative Strategy, 12*(2), 141–165.

Arquilla, J. (2012). Cyberwar is already upon us: But can it be controlled?. *Foreign Policy Magazine*, Retrieved from http://www.foreignpolicy.com/articles/2012/02/27/cyberwar_is_already_upon_us

Carr, J. (2010). *Inside cyber war.* Sebastopol, CA: O'Reilly Media.

Clarke, R. A., & Knake, R. K. (2010). *Cyber war: The next threat to national security and what to do about it.* New York: HarperCollins Publishers.

Lewis, J. A. (2013, February). "Conflict and Negotiation in Cyberspace." Washington, DC: Center for Strategic and International Studies (CSIS).

Libicki, M. C. (2009). *"Cyberdeterrence and cyberwar."* Santa Monica, CA: RAND Corp, Prepared for the Air Force.

Libicki, M. C. (2007). *Conquest in cyberspace: National security and information warfare*. New York: Cambridge University Press.

Rid, T. (2013). *Cyber war will not take place*. New York: Oxford University Press.

Singer, P., & Friedman, A. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. New York: Oxford University.

Von Clausewitz, C. *On war*. Ed. and Trans. By Michael Howard and Peter Paret. Princeton, NJ: Princeton University Press, 1984.

AUTHOR

Matthew J. Flynn (mflynn92@gmail.com) accepted a faculty position with the Command and Staff College, Marine Corps University in July 2012. He has taught at a number of universities and most recently served as assistant professor at the United States Military Academy, West Point, in both the Military and International Divisions of the History Department. Flynn is a specialist in comparative warfare of the U.S. and the world. His publications include a recent co-authored study titled *Washington & Napoleon: Leadership in the Age of Revolution* (Potomac Books, 2012), and books such as *First Strike: Preemptive War in Modern History* (Routledge, 2008), and *Contesting History: The Bush Counterinsurgency Legacy in Iraq* (Praeger Security Int., 2010). Together these works examine a wide range of foreign policy issues across time and in a global context. Flynn received his PhD from Ohio University in 2004 after advanced study in civil-military relations with OU's distinguished Contemporary History Institute. His general areas of interest are great power status, preemptive war, cyber warfare, and piracy.

Cyber Warfare Simulation to Prepare to Control Cyber Space

Martin R. Stytz | Sheila B. Banks

ABSTRACT

Cyber space is increasingly dynamic, uncertain, and complex. A cyber attack can be used to control an adversary's information, target the portions of cyber space used for situational awareness and decision-making, as well as lead the adversary to make desired decisions. A cyber attack diminishes individual and group situational awareness and command and control by undermining one or more elements of cyberspace. Exposing decision-makers to cyber warfare using simulation can prepare decision-makers for the challenges posed by cyber conflict. Due to the importance of cyber space to success in warfare, techniques both for proper assessment of real-world and cyber circumstances and for achieving strategic defensive cyber dominance must be trained via exposure to simulated cyber attacks. As a step toward addressing these current and future cyber space defense challenges, we propose using a data/situational awareness-based orientation for assessing tactical and strategic cyber offensive and defensive activities. Using the proposed orientation, it is evident that: (1) accurate simulation of cyber warfare will be a useful tool for preparing decision-makers for cyber conflict, and (2) a well-constructed cyber attack diminishes individual and group situational awareness and command and control by undermining one or more elements of cyberspace.

A data/situational awareness-based orientation reveals that we need only alter the information presented to the decision-makers to simulate a cyber attack. Therefore, appropriately configured simulation environments can be used to develop expertise in dealing with cyber conflicts and provide an environment for the development of cyber conflict strategies and tactics. This paper introduces the challenges of situation awareness and the role that simulation can play to research, develop, and integrate cyber space defense strategies.

INTRODUCTION– CYBERSPACE

A great part of the information obtained in War is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character. …this is not a trifling difficulty even in respect of the first plans,…but it is enormously increased when in the thick of War itself one report follows hard upon the heels of another.

Clausewitz, On War (Clausewitz, 1968, 1908 translation)

Dependence upon information technologies and networks (Alberts and Hayes, 2003; Geer and Archer, 2012) provides both a new avenue for acquiring important information during a conflict and creates a new target for attack (Alberts and Hayes, 2003; Geer and Archer, 2012). By using a cyber attack, it is possible to control an adversary's information,

target the portions of cyber space used for situational awareness and decision-making, lead the adversary to make desired decisions, and directly affect the opponent's decision processes and situational awareness. Using a cyber attack, it is possible to lead an adversary to make the decisions that we desire and to confuse an adversary. The breadth, complexity, and pace of improvement in cyber space technologies (Lynn, 2010; Acquisti, and Grossklacs, 2005; Cook and Pfleeger, 2010; Giffin, 2010; Hole and Netland, 2010; Johnson, and Pfleger, 2011; Kenney and Robinson, 2010; Schiffman, Moyer, Jaeger, McDaniel, 2011; Stone-Gross, et.al. 2011; Skoudis and Zeltser, 2003; Graham and Maynor, 2006; Levine, Grizzard, and Owen, 2006; Naraine, 2006; Rutkowska, 2005) indicates that the challenges posed by a cyber attack may overwhelm decision-makers when they first experience such an attack. Therefore, decision-makers should be prepared for the environment they will encounter in cyberspace; this can be achieved by the use of accurate cyber attack simulations. In this paper, we discuss the informational aspects of a cyber attack and present an approach for preparing decision makers for cyber attack's effects using a simulation environment to prepare decision-makers to conduct strategic cyber defensive operations by exploiting virtual machine technology and defensive cyber space situational awareness.

In the conception employed, *cyberspace* is composed of four main elements, as illustrated in Figure 1: 1) *data*, 2) *computing technologies* (such as computer hardware, computer software, computer networks/infrastructure, network protocols, virtualization, and cloud computing), 3) *information analysis/comprehension technologies* (such as information visualization, collaboration, and data mining technologies), and 4) *information interaction/management technologies* (such as human-computer interaction, intelligent agent technologies, human intent inferencing, personalization technologies, and database technologies.) A cyber attack is an attack upon one or more of these four elements.

Preparation to defend oneself in cyber space is increasingly urgent because cyber attacks of all types continue to increase in sophistication (Lynn, 2010; Acquisti and Grossklacs, 2005; Cook and Pfleeger, 2010; Giffin, 2010; Hole and Netland, 2010; Johnson, and Pfleger, 2011; Kenney and Robinson, 2010; Schiffman, Moyer, Jaeger, and McDaniel, 2011; Stone-Gross, et.al. 2011; Skoudis and Zeltser, 2003; Graham and Maynor, 2006; Levine, Grizzard, and Owen, 2006; Naraine, 2006; Rutkowska, 2005), which in turn undercut the usefulness and value of data and the other cyber space elements for decision making and situational awareness (Delquié, 2008; Kangas, 2010; Lumsden and Mirzabeiki, 2008; Oppenheim et.al., 2003a; Oppenheim et.al., 2003b; Oppenheim et.al., 2003c; Shepanski, 1984). This increase in sophistication has been clearly demonstrated by the Stuxnet, Flame, Red October, and DuQu malware deployments. The challenges posed by increasingly capable malware are compounded by the introduction of virtual machine technologies (as discussed in NIST 800-125), and cloud computing technologies (Graaido, Schlesinger, and Hoganson, 2013; Takabi, Joshi, Ahn, 2010; Liu, Weng, Li, Luo, 2010; Krutz, and Vines, 2010; Cachin and Schunter, 2011; Krutz and Vines, 2010; Jamsa, 2013). The combination of the malware and the virtual machine and cloud computing technologies indicates that a reassessment of modes of information protection and the associated reasoning about protection of data and computational resources during an attack is required. Future malware attacks will, inevitably, target systems in the same sophisticated manner as Stuxnet, by transmitting data from the targets and/or subtly modifying the data so as to corrupt it in a malicious, but not immediately apparent, manner. We expect that future cyber attacks will be structured to support the introduction of false information, to target individuals for information degradation, and to precisely corrupt information that reaches decision-makers. Cyber attacks will be coordinated and mounted in campaigns in order to maximize confusion and maximally exploit cyber successes. Strategic as well as tactical expertise in managing dynamic, adaptive responses to cyber attacks will be crucial to successful cyber defense and to maintaining strategic defensive cyber dominance.

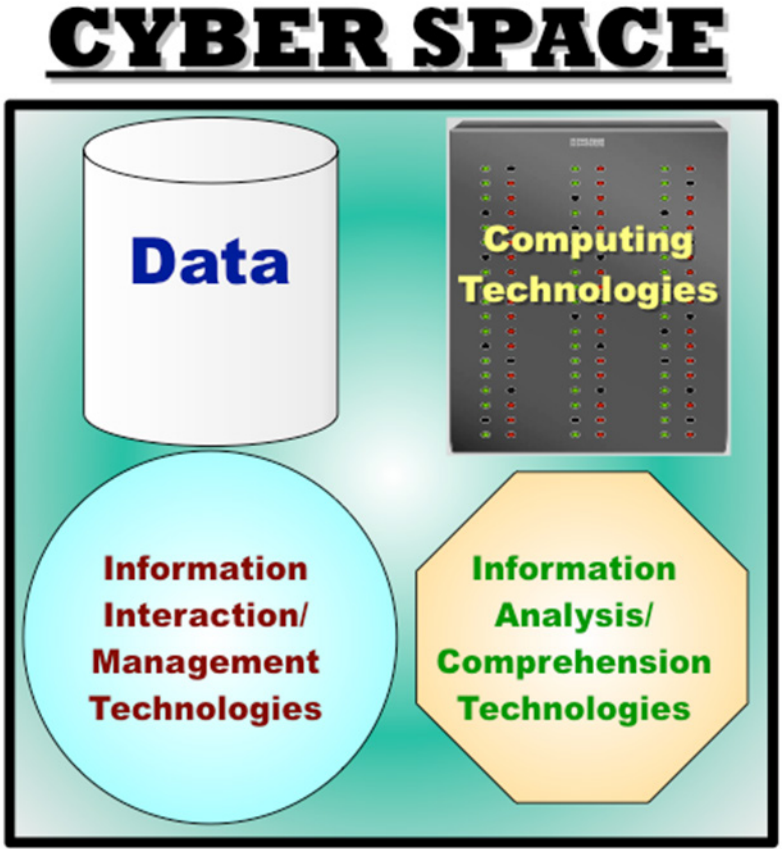

FIGURE 1: THE FOUR ELEMENTS OF CYBER SPACE.

Strategic offensive cyber dominance exploits adversary biases by a combination of data exfiltration and manipulation to lead the adversary to make decisions that we want them to make and undercut an opponent's effective decision-making and mission command. Strategic cyber offensive targeting should be based upon the desired effects on the data and decision processes of the opponent and not upon the material damage that may, or may not, be inflicted. Conversely, *strategic defensive cyber dominance* enables effective decision-making for one's own side. It ensures accurate, trustworthy, relevant data is provided to friendly decision-makers. The vast amount of open-source cyber attack literature demonstrates that no combination of tactical cyber defense technologies is impervious. Therefore, one's own systems and decision-makers must be prepared technologically and psychologically to function despite strategic cyber attacks designed to undermine situational awareness, decision-making ability, and mission command. Strategic cyber defense dominance arises from a combination of tactical cyber defense technologies, a resilient cyber defense system architecture, and decision-maker preparation for psychological effects of a strategic cyber attack. Decision-maker strategic cyber defense preparation requires training via exposure to the effects of cyber attacks so the decision-maker can surmount the challenges posed to situational awareness and decision-making by a strategic cyber attack.

Strategic cyber defense dominance enables situational awareness and effective, trustworthy decision-making (Lynn, 2010). Strategic cyber defense dominance further ensures that accurate, trustworthy, relevant information is provided to the decision-makers. Because strategic cyber defense

dominance is not assured, systems and decision-makers must be prepared for cyber attacks designed to undermine situational awareness, decision-making ability, and mission command. There are two needs that the preparation must address. The *first* is to prepare decision-makers for the confusing, contradictory, and misleading information that will be presented to them during a cyber attack. The *second* is preparing decision-makers to exploit cyber space dominance by effective employment of trustworthy information analysis/comprehension, and information interaction/management technologies.

Simulation environments allow us to prepare decision-makers for the inevitable cyber attacks upon the information they need for decision-making, to develop skill in achieving and retaining strategic cyber defense dominance, and to develop cyber defense experience, strategies, and tactics that preserve information value and insure that decision-relevant information reaches decision-makers. Training in effective cyber response is imperative because uncertainty, confusion, and information overload (the three objectives of cyberattackers) are known to lead to improper and counter-productive human behaviors. Because of the volume of information that must be considered and the rapid pace of activity in the cyber battlespace, the decision-maker and decision support personnel must be prepared for the confusing and novel information circumstances that will occur.

The tools, techniques, and training needed to prepare decision-makers for the challenges of cyber conflict must address three classes of cyber situations: 1) operations during normal conditions, 2) operations during a cyber attack, and 3) operations after a cyber attack. These tools, techniques, and training may be developed using simulation environments designed to achieve the following goals: 1) improve understanding of the challenges posed to decision-makers during a cyber attack, 2) test and evaluate the cyber defense strategies, tools, techniques, and training, 3) practice using cyber defense tools and techniques, and 4) determine information value during a wide array of circumstances in order to deploy cyber defenses. The tools, techniques, and training must be extensible and flexible so that they can be readily altered to address new cyber threats and tactics.

BACKGROUND

Two crucial elements for the development of simulation environments are situational awareness and virtual machine technology.

Situational Awareness

The development of information technologies, network centric warfare (Alberts and Hayes, 2003), and modern electronic networking technologies has given rise to the belief that military staffs will quickly develop a shared correct situational awareness that will greatly facilitate decision-making, thus permitting faster response to challenges by reducing the complexities of the military administrative and command structure. A cyber attack undercuts these assumptions for the individual and groups.

The concept of situational awareness is not well defined, but much research has been devoted to determining the process by which it arises (Boytsov and Zaslavsky, 2011; Endsley, 1995a; Endsley, 1995b; Endsley, 2000; Gerken, et.al., 2010; Guang and Chang, 2011; Holsopple, et.al., 2010; Jones, Connors, and Endsley, 2011; Lan, Chunlei and Guoqing, 2010; Ma and Zhang, 2008; Mihailovic, et.al., 2009; Nwiabu, et.al. 2011; Parvar, Fesharaki, and Moshiri, 2010; Rahman, 2011; Stanton, Salmon, Walker, Jenkins, 2010; St. John and Smallman, 2008; Vachon, et.al., 2011; Xi, Jin, Yun, Zhang, 2011; Osinga, 2005). There is some agreement on what situational awareness is: situational awareness is the result of a dynamic process of perceiving and comprehending events in one's environment, leading to reasonable projections as to possible ways that the environment may change, and permitting predictions as to what the outcomes will be in terms of performing one's mission (illustrated in Figure 2). There is also some agreement on what constitutes shared situational awareness and how it develops via a process of integrating the mission-essential overlapping portions of the situational awareness of individual team members—thus,

developing a group dynamic mental model of the battlespace (Endsley, 1995a; Endsley, 1995b). For the purposes of our discussion, we adopt Endsley's definition (Endsley, 1995a; Endsley, 1995b). Endsley defines situational awareness (SA) as: the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, the projection of their status into the near future, and the prediction of how various actions will affect the fulfillment of one's goals. Endsley identifies four components of situational awareness, PERCEPTION (what are the facts), COMPREHENSION (understanding the facts), PROJECTION (anticipation based upon understanding), and PREDICTION (evaluation of how outside forces may act upon the situation to affect your projections). These components are not stages, but instead interlocking cycles that progress in relation to each other. Factors promoting individual SA are both structural and situational. Structural factors include background, training, experience, personality, interests, and skill, as well as situational factors that include the mission that is being performed and the prevailing circumstances. Several factors are known to cause degradation of individual situational awareness, including: 1) ambiguity (arising from discrepancies between equally reliable sources), 2) fatigue, 3) expectations and biases, 4) prior assumptions, 5) psychological stress, 6) misperception, 7) task overload, 8) boredom (not enough to do on the tasks to maintain focus), 9) information shortage, 10) information overload, 11) information interruption, 12) irrelevant information, 13) mission complexity, 14) fixation/attention narrowing, 15) erroneous expectations, and 16) lack of experience.

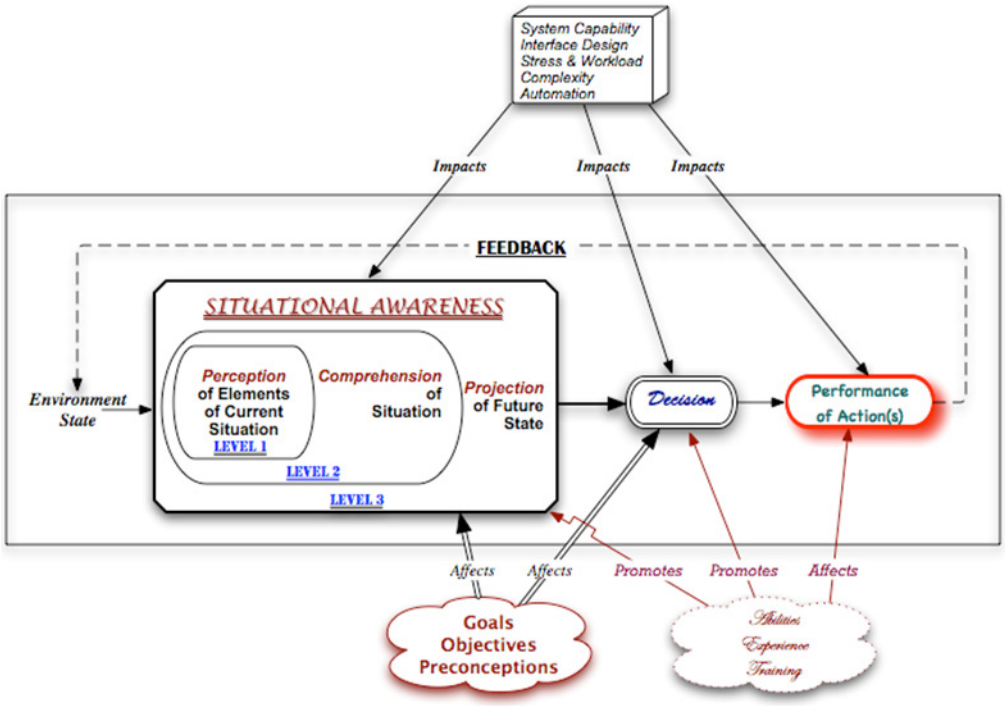

FIGURE 2: THE SITUATIONAL AWARENESS CYCLE BASED ON (ENDSLEY, 1995A; ENDSLEY, 1995B).

Shared situational awareness can be defined as a common relevant mental model of a distributed environment or the degree to which one individual's perception of current environment mirrors the situation as perceived by others. Shared situational awareness benefits from information superiority and a flexible and interoperable information picture, but relies upon communications in order to share information. Shared situational awareness can provide a common operational picture, which means that the members of a team share essentially the same near-real-term mental model of the environment. Shared situational awareness ensures that a clear and accurate, common, relevant mental model of the environment is possessed by leaders at all levels. Shared situational awareness also provides a common comprehension of relevant policy and strategy as well as the state of operations, technology, logistics, tactics, plans, command structure, personalities, and readiness posture. By improving and augmenting tools for shared and individual situational awareness, we can increase the ability to develop situational awareness in crisis situations and better assess an enemy's situational awareness of our state. As with individual situational awareness, there are many factors that are known to degrade shared situational awareness, including: 1) false group mindset, 2) the "press on regardless" mindset (allowing mission accomplishment to affect objective assessment), 3) insufficient training/variable skill levels, 4) poor personal communications skills, 5) perception conflicts, 6) frequent changes in personnel, 7) degraded operating conditions, 8) lack of common information across the group, and 9) the absence of non-verbal cues. In general, distributed workers have less overlap in their mental models than do co-located workers.

Virtual Machine Technology

A virtual machine, illustrated in Figure 3, is software that creates a virtualized environment between the computer platform and its operating system, so that software (including an operating system) can execute on an abstract machine (Bernstein and Vij, 2010; Adair, Bayles, Comeau, Creasy, 1966; Amdahl, Blaauw and Brooks, 1964; Barham, et.al., 2003; Case and Padegs, 1978; Creasy, 1981; Doran, 1988; Daley and Dennis, 1968; Fabry, 1973; Fraser, Hand, Pratt, Warfield, 2004; Gifford and Spector, 1987; Goldberg, 1974; Gum, 1983; King, Dunlap, and Chen, 2002; Lampson and Sturgis, 1976; Laureano, Maziero, and Jamhour, 2004; Lett and Konigsford, 1968; Shapiro, Vanderburgh, Northrup, Chizmadia, 2004; Meyer and Seawright, 1970; Peterson, Silberschatz and Gagne, 1983-2004; Popek and Goldberg, 1974; Popek and Farber, 1978; Seawright and McKinnon, 1979; Uhlig, et.al., 2005). A virtual machine is a software-based impersonation of a computer. A virtual machine presents the illusion of the real computing machine to a user and associated software. In a virtual machine, all components of a given computer hardware/operating system combination are replicated within a host operating system to provide the computational illusion that all applications executing within the virtual operating system are running on the original software/hardware combination hardware; however, it is simply an illusion. A virtual machine does not add functionality to the operating systems (and applications within them) that it hosts but instead provides functionality and a software interface to them that is identical to the replicated system and also controls communication between the virtual machines. In this environment, there is complete protection of all actual system resources and hardware from each of the virtual machines; each virtual machine is also isolated from all other virtual machines. Communication between virtual machines is possible, and is usually patterned upon network communication. Achieving a virtual machine capability requires the use of technology for management of virtual processors, virtual storage, virtual memory, and virtual I/O devices.

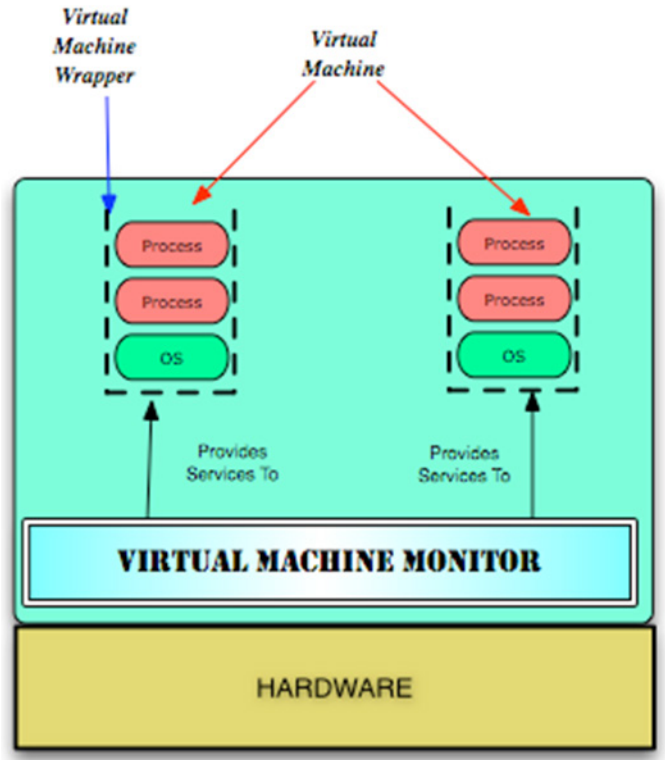

FIGURE 3: VIRTUAL MACHINE ARCHITECTURE.

The supervision and oversight of executing software in each virtual machine (VM) are performed by the virtual machine monitor. The virtual machine monitor (VMM), sometimes referred to as a hypervisor or virtualization manager, is a program that allows multiple operating systems—which can include different operating systems or multiple instances of the same operating system—to share a single hardware processor. A VMM is usually designed for a particular CPU architecture. When running under the control of a hypervisor, each operating system on a computer appears to have a dedicated processor, memory, and other computing resources. However, the VMM actually controls the real processor and its resources, allocating and scheduling them for each operating system in turn. Because an operating system is often used to run a particular application, or set of applications, in a dedicated hardware configuration, the use of a VMM makes it possible to run multiple operating systems (and their applications) within a single computer architecture.

There are three technologies needed to assemble a virtual machine: virtual memory, software emulation, and context switching. With these technologies, it is possible to build a host operating system that can provide virtual machine capabilities to any given guest operating system. In 1974, Popek and Goldberg defined the formal necessary conditions for achieving a virtualizable computer architecture (Popek and Goldberg, 1974). For any computer a virtual machine monitor may be constructed if the set of sensitive instructions for that computer is a subset of the set of privileged instructions. In other words, the most essential requirement that the computer architecture must exhibit in order to be "virtualizable" is that privileged instructions must trap. This requirement means that when a

guest virtual machine (while running directly on the real processor) attempts to execute a privileged instruction, the processor halts instruction execution and returns software program execution flow control to the virtual machine monitor (VMM) so that the VMM can decide whether or not to execute the instruction or simulate execution of the instruction by some other means. Furthermore, Popek and Goldberg determined that a true virtual machine architecture must exhibit three essential characteristics (Popek and Goldberg, 1974). The first characteristic is that any program run under the VMM should exhibit behavior identical with what would be observed if the program had been run directly on the original machine. They offered one exception to this rule: timing. Execution in a virtual machine can be slower than it would be on the actual machine. The second characteristic is that a statistically dominant subset of the virtual processor's instructions execute directly on the real processor. The third characteristic is that the VMM is in complete control of system resources. A virtual machine running on the system does not have direct access to any of the system's real resources; it must go through the VMM, which means that all behaviors and instructions executed by a virtual machine on the computer can be monitored and halted or modified as necessary.

SIMULATION FOR ACQUIRING CYBER DEFENSE EXPERIENCE

As the technical sophistication of cyber attacks increase, the old modes of information protection and reasoning about data protection during an attack must be re-assessed, and approaches for achieving strategic cyber defense dominance must be developed. Simulation provides a safe and flexible way to prepare decision-makers for the challenges of cyber attacks as well as to re-assess data protection techniques and cyber defenses. To be useful as cyber attack technologies evolve, cyber simulation must portray cyber attack and defense actions in a manner that corresponds to human perceptions of them. Therefore, the simulation must capture and represent the activities of the decision-maker and staff, the attacker and defender goals, the sequence of operations that the attacker will execute, the activities of the cyber defender, logical and physical data location(s), and the potential responses of the attackers and defenders to each other's actions. In previous work, we presented a technique for cyber simulation that can be used to model cyberoperations, its components, and the possible responses to defensive actions (Stytz and Banks, 2006a; Stytz and Banks, 2006b; Stytz and Banks, 2004). The same simulation approach can be used to develop procedures for cyber defense training.

To prepare decision-makers for cyber conflict, there are four key training considerations: 1) teaching how to determine the targets of attacks; 2) teaching the techniques and tactics likely to be used against targets; 3) teaching techniques and tools that should be used to counteract each type of attack and its concurrent effects; and 4) teaching means for explicitly assessing information value and targeting cyber defenses to protect the highest value information. Cyber simulation can be used to achieve these four goals. To minimize the cost of the development of cyber simulation environments, we couple existing simulation systems with cyber simulation systems that provide effects of cyber simulation and cyber attack upon the existing simulation systems, as illustrated in Figure 4. To create cyber simulation environments that impart the required cyber defense knowledge and experience, the components of the cyber simulation systems must exchange information about the attack and defense, the status of the cyber event, and portray the results of the cyber attack and defensive responses.

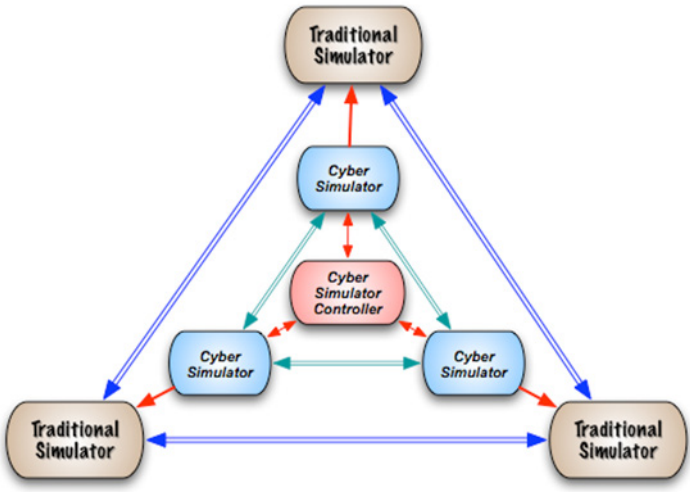

FIGURE 4: CONCEPTUAL CYBER SIMULATION ENVIRONMENT.

The key to our approach is the insight that to simulate a cyber attack, we need only affect the information presented to the decision-makers. To affect the information, there are three approaches that we can use: 1) an increase in information presented, 2) blocking information needed by a user, and 3) substituting false information for the actual information requested by the user. In all cyber attacks, the actual target is the human operator's ability to make an effective decision, thus increasing the decision-maker's decision uncertainty. There are two central problems that a decision-maker faces: 1) determining which information to use to make a decision, and 2) determining when the information in hand does not permit a decision to be made based upon the information. This second problem is well-known and occurs in many situations, yet it persists and only training can equip a decision-maker with the experience and expertise needed to recognize either situation. The second problem is especially treacherous because it leads to a decision-maker taking the wrong action or no action at a critical moment. To prepare the decision-maker for the information issues that will arise during different types of cyber attacks, a few general techniques can be employed. During the simulation situation, the decision-maker can be given an overwhelming amount of information, denied information, given a mixture of accurate and false information, or a mixture of these techniques that may vary over time.

Cyber attack simulation uses cyber simulation systems in conjunction with existing simulation hosts. The cyber simulation system must perform three key tasks: 1) determine if a cyber attack is successful, 2) determine the effect of the cyber attack upon each host and its data, and 3) portray defensive responses to the cyber attack. In our approach, each host has a cyber simulator that services it and provides these capabilities. The cyber simulator provides each host with the inputs needed to portray the effects of simulated cyber attacks. Because each cyber simulator services only one simulation environment host, the cyber simulators communicate with each other using a logically separate cyber simulation network. The approach requires two logical, but separate, communications networks. One logical network links the simulation systems that form simulation environments identical to those in use today. The second logical network links the cyber simulators and is used to exchange data concerning cyber attacks and defensive responses to

the cyber attacks. Each cyber simulator is connected to a simulation environment host, allowing the cyber simulator to control the information presented by the host so that the data available to decision-makers will approximate the information available to them in a real-world cyber event.

To simulate cyber events, we use the cyber simulators to compute the probability that the cyber attack would penetrate the host's simulated cyber defenses and, if the attack is successful, the initial state for the cyber attack that the host system should enter. Cyber attack probabilities are computed by combining the historical success rate for similar cyber attacks upon similar target systems combined with a weighting for desired success rate for cyber attacks within the simulation and a weighting for the desired success rate for the same class of cyber attacks within the simulation. After computing the initial state for a successful cyber attack, the cyber simulator then advances from state to state in the attack and drives its host systems through the appropriate information availability states as determined by the state of the simulated cyber event. At each step of the cyber attack and defensive response, the decision-makers are provided with indications of the status of the attack and information behaviors that mirror the delays and alterations that would occur in the corresponding real-world attack. The status of the cyber attack, the status of the cyber defense, the information behaviors, the defenders' strategy and tactics, and the defenders' situational awareness provide the decision-making context, all of which must be simulated and provided to hosts and users. In our simulation approach, changes to the cyber defense that increase or decrease its depth are reflected in increased or decreased delays in information movement through the systems. To employ this approach, each cyber simulation system computes an identical representation for the progression of the cyber event based upon the initial description of the cyber attack and the associated probability for transition from state to state in the cyber attack. To keep the cyber control message size reasonable, we pre-position the states for the cyber events at each cyber simulator. Determining the states and documenting them in a manner that a computer can use is accomplished using the Unified Modeling Language (UML) (Albir, 1998; Booch, Rumbaugh and Jacobson, 1999).

Because the cyber simulators communicate between themselves to exchange information, shared information includes the type of cyber attack being simulated, the defenses that are present, the cyber defenses that have been activated, the status of cyber defenses, the probability of success of the attack (given the defenses and defensive response), and the variations of the cyber attack that are being simultaneously launched. Other information that needs to be shared and would typically come from the simulation cyber controller includes data sources to be interfered with, the probability of success for interference with each source, the types of data from each source to be corrupted, the probability of data corruption, the frequency of corruption, and techniques for corruption for each type of data from each source. Additional information provided by the cyber simulator controller includes the types of data from each data source to be faked/inserted into the data stream, the probability of a successful insertion, the frequency of data insertion, the types of data to be inserted instead of the actual data, the types of data from each data source to be blocked, the probability of success for each attempt at blockage, the frequency of attempts for blockage, and the length of each successful blockage. Additional cyber simulator control and response information can be encapsulated, at a minimum, within a few probability statements transmitted from the cyber simulator controller to the cyber simulators and, as the cyber simulation capabilities improve, the information that is exchanged can be elaborated upon so that the cyber simulation can increase its sophistication.

The probabilities for the success and progress of a cyber attack can be derived using a combination of assessments of the vulnerability of the software being attacked and the historical likelihood of success of similar attacks as computed using statistics gathered by the various computer attack response agencies and the National Threat Database.

DIMINISHING CYBER ATTACK EFFECTIVENESS

Diminishing the effectiveness of cyber attacks results in improved protection and use of the elements of cyber space (data, computing technologies, information analysis/comprehension technologies, information interaction/management technologies) in order to minimize the opportunity for surprise and exploitation of surprise. To diminish the effectiveness of the cyber attack and, thereby, preserve usable SA and integrity for the elements of cyber space requires training in assessing and counteracting cyber attacks and their effects upon decision-making as well as a different approach to layered defense of systems and applications. The distributed environment training environment architecture allows us to prepare decision-makers to defend cyber space, to prioritize information, to prioritize the elements of cyber space, and to operate in a cyber conflict wherein some cyber space elements, especially data, are compromised to an uncertain degree.

CYBER DEFENSE TECHNOLOGY CONSIDERATIONS

Because any cyber defense can and will be defeated, our cyber defense goals are the following: 1) to make defeating a cyber defense as difficult as possible, 2) to provide cyber defenders with dynamic defenses, 3) to provide cyber defenders with a foundation for the development of tools for rapid detection of cyber attacks, 4) to enable cyber defenders to successfully operate despite a breach in cyber defenses, and 5) to provide an environment that enables rapid recovery from cyber penetration and compromise. To complement these technical goals, we require a means for identifying, modeling, and prioritizing the key components of each element of cyber space in any decision context. To model the relative priorities of each of the components of the four elements of cyber space we use protection rings. For cyber defense, the rings correspond to priorities for information protection and can be used to guide strategic cyber defense resource allocation as well as tactical decisions to isolate systems or subsystems that are compromised. Rings closer to the center of each element's ring conceptually contain components of that cyber space element that are of greater value, importance, and usefulness to the decision context at hand. The number of rings and the content of each ring are determined by the decision-making context. We use one set of rings for each element of cyber space. Each ring for each cyber space element contains information of approximately the same importance for a decision-making context. Therefore, to simulate a cyber attack we alter the specific information needed in a decision-context by modifying the information content of specific rings for those elements that are to be compromised by the cyber attack. The type of cyber attack, the cyber defenses, the expertise of the decision-maker, and the learning outcome(s) for the simulation exercise determine the number of rings affected for each element and the value of the element's components that are altered.

In our approach, we determine which information rings are compromised using the probability that the simulated cyber defenses that protect the information in each ring can be compromised. These probabilities are based upon the operations and outcomes of similar real-world cyber attacks. To determine which information in a compromised ring to alter, the simulation environment maintains a record of the cyber attacks that have succeeded as well as the decision-making context faced by the decision-maker in the simulation environment. The information content in a ring is typically determined by the simulation environment, but users or instructors can intervene to alter information ring placement. The vulnerability of a ring and the information in a ring are the two pieces of information used to compute an estimate of the likelihood that the cyber attack can alter, destroy, or falsify each component of a compromised ring. The cyber controller then simulates the required change and passes the result on to its simulation host. To enhance realism, not all of the information of equal importance to a decision context (i.e., in the same ring) is altered, only some of the information in each affected ring is changed.

ACTIVE CYBER DEFENSE

As evidenced by the continued increase and severity of cyber defense breaches, current approaches to cyber defense are minimally effective. Furthermore, in light of foreseeable developments in malware capabilities, we suggest that the current ***static*** *cyber defense-in-depth* is unviable in the face of the continuing emergence of cyber attack capabilities. The challenges faced by cyber defense points to the need for the use of *dynamic adaptive layered cyber defense* technologies (DLCD). DLCD is designed to isolate malware infestations and to maintain sufficient, accurate, and trustworthy cyberspace elements throughout the organization in spite of the attack, ensure mission accomplishment, and give decision-makers sufficient time to recognize and counteract the attack. Figure 5 illustrates the approach for a single element of cyberspace. In DLCD, each element of cyber space is protected by one or more virtual machines. Clearly, virtual machine nesting requires relaxation of Popek's second characteristic of a virtual machine (Popek and Goldberg, 1974; Popek and Farber, 1978). VM nesting provides the capability to protect one or more components in each element with additional virtual machines with an ever-increasing number of privileged instructions as warranted by the threat and importance of the component to the current decision. The successive layers of VM layering for an element have increasingly restrictive, i.e., broader, sets of privileged instructions and may even have no non-privileged instructions. The number of rings in a cyber space element and the number of virtual machines deployed to protect the element and its components are not correlated, the allocation of virtual machines for cyber defense is a decision made by human decision-makers. The number of virtual machines is constrained by the performance desired by the user(s). By using multiple virtual machines to protect each of the elements of cyber space, the approach supports dynamic allocation of cyber defense resources, either by adding additional virtual machines to the protection of an element or component, altering the virtual machine mix, or by changing cyber attack detection systems within each virtual machine for an element. We use estimates to compute the probabilities for cyber attack success. In future work, we will use historical data and simulation outcomes to improve the probabilities.

By using a multi-layered virtual machine approach, the defense can take the initiative in responding to a cyber attack while the attack is in progress. For example, if a virtual machine, element, or component is compromised, a portion of it can be selectively abandoned and cyber defense shifted to protect the portions that have not been infected. The compromised portion can also be restarted in a more secure environment from a safe, infestation-free state. DLCD allows for flexible protection of cloud and virtual machine resources as well as data. A cyber simulation environment can prepare decision-makers to manage a dynamic layered cyber defense.

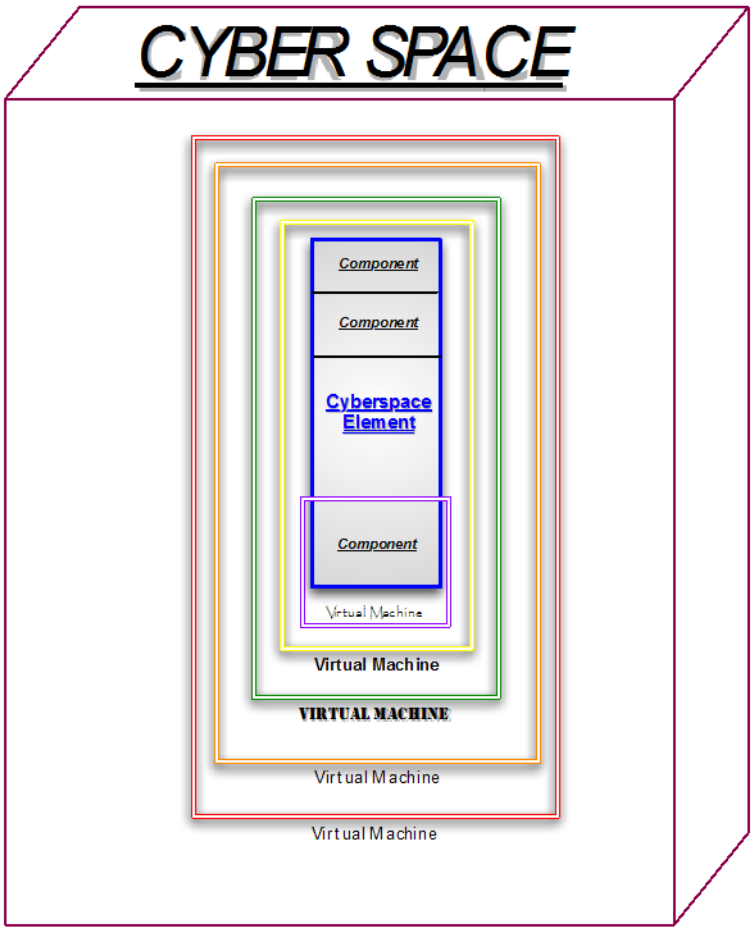

FIGURE 5: NOMINAL DYNAMIC CYBER DEFENSE ARCHITECTURE FOR AN ELEMENT.

A crucial challenge that the cyber defender must address is how to protect the elements of cyber space, especially important information, during cyber attacks without imposing an unacceptable delay upon information delivery while preserving the value of information relative to the decisions to be made (Delquié, 2008; Kangas, 2010; Lumsden and Mirzabeiki, 2008; Oppenheim et.al., 2003a; Oppenheim et.al., 2003b; Oppenheim et.al., 2003c; Shepanski, 1984). The importance of timely and accurate information delivery is hard to overstate; delay leads to incorrect decisions, failure to make decisions, and failure to gain or maintain situational awareness. Further compounding the information delivery challenge is the need to share information in order to develop and maintain group situational awareness; in current and future cyber space there are generally many decision-makers involved in the information assessment and decision process in every choice. While information increases in value when it is shared, the sharing process also increases the vulnerability of the information, the decision support tools, and the decision-making process itself. As a result, when decision-makers are assessing cyber space protection strategies they must not only consider how to protect cyber space and the information they require, but how to protect the same information as it is delivered to all others involved in the same decision.

In our approach, the cyber conflict training challenge is twofold. First, decision-makers must learn how to assess the metrics for each element, as no one metric can provide evidence of a cyber attack or successful cyber defense. While artificial intelligence can be employed to aid the decision-maker, there are no substitutes for human judgment, the ability to maintain situational awareness, and the ability to correlate disparate activities into insight concerning the state of a cyber space element. The second challenge is that human decision-makers must learn how to substantiate or refute their theories concerning the cyber security state of a given element. Due to the complexity of these two challenges, simulation of cyber conflict is a practical method for acquiring the necessary expertise and familiarity with cyber activities, threats, and symptoms to develop and maintain cyber space situational awareness.

The pursuit of cyber space situational awareness is undertaken to secure cyber space and to attain situational awareness in the other parts of the battlespace: air, ground, sea, and space. Because this situational awareness for the individual and groups is so important, training environments designed to provide experience and expertise in addressing cyber space situations are important. However, because of the number of variables involved in assessing the state of cyber attacks and cyber defenses, decision-makers cannot be expected to determine the state of each sub-component of each cyber space element and assess their validity during the press of events. Instead, displays for state, interfaces to support interaction and assessment of the interfaces, and displays that provide indication of the validity of the data are required. To maximize their effectiveness, decision-makers must be able to concentrate on cyber space situational awareness and cyber space status challenges without the distractions of computing and validating the metrics that they use for situational awareness and decision support.

SUMMARY

By the word information we denote all the knowledge which we have of the enemy and his country; therefore, in fact, the foundation of all our ideas and actions.

Clausewitz, *On War* (Clausewitz, 1968, 1908 translation)

The threats posed by technically sophisticated cyber attacks are increasing. Few penetrations are detected while they are underway, most are detected only after the malware is implanted and damage to the elements of cyber space has attained a noticeable level. Possessing cyber superiority will not guarantee victory for a network-centric force, but the lack of cyber superiority will almost certainly ensure the defeat of a network-centric force. While deception and information denial operations are techniques as old as warfare itself, technically sophisticated cyber attacks permit, for the first time, a wide-scale, persistent, and virtually undetectable attack upon the information, tools, and other elements of cyber space that a decision-maker employs to make a decision. The technically sophisticated cyber attack will undermine information, surprise decision-makers, generate confusion, forestall situational awareness development, and corrupt decision-making. As a result, tools for training decision-makers to cope with cyber attacks coupled with architectures that support real-time alteration of cyber defenses, using virtual machine and cloud computing environments, are needed. The complexity of future cyber systems will continue to increase, as witnessed by the development of intercloud technologies (essentially a cloud of clouds and smart grid technologies for remote control and management of real-world infrastructure) which increases the complexity of cyber attacks and creates new vectors for executing cyber attacks.

In this paper, we discussed the need for cyber defense training environments for decision-makers. The network and associated software will become increasingly important and lucrative targets for adversaries and we must be prepared to counter their cyber attacks. Therefore, decision-makers and

information technology specialists must be trained to recognize and counteract a cyber attack against critical information resources early in the attack. The key to the requisite training is the development of simulation environments that impart the experience and expertise needed to make effective cyber defense possible in the face of cyber attacks. We described a means for presenting the effects of cyber attacks to decision-makers to prepare them for the challenges of cyber conflict.

Our next efforts will address the question of simulating complex cyber attacks and cost effective, but accurate, provision of training services. More broadly, research targeted at advancing cyberbattle understanding and defender decision-making during a cyber attack is needed. We must also gain a better understanding of decision-making and situational awareness within large-scale and high-volume data environments that have noise and uncertainty inherent in the data, as well as due to cyber attacks. Additionally, we will work to improve our ability to determine the probability of a successful cyber attack in light of multiple layers of virtual machines and multiple, simultaneous cyber attacks.

REFERENCES CITED

Acquisti, A. & Grossklacs, J. (2005, January–February). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*(1), 26–33.

Adair, R. J., Bayles, R. U., Comeau, L.W., & Creasy, R. J. (1966, May). A virtual machine system for the 360/40. Cambridge, MA*: IBM Scientific Center Report 320-2007*.

Alberts, D. S. & Hayes, R. E. (2003). *Power to the Edge.* Washington, DC: CCRP Press, CCRP Publication Series.

Albir, S. S. (1998). *UML in a Nutshell.* Sebastopol, CA: O'Reilly Press.

Amdahl, G. M., Blaauw, G. A., & Brooks, F. P. (1964). Architecture of the IBM system/360. *IBM Journal of Research and Development, 8*(2), 87–101.

Barham, P., Dragovic, B., Fraser, K., Hand, S., Harris, T., Ho, A., Neugebauer, R., Pratt, I., & Warfield, A. (2003, October). Xen and the art of virtualization. *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP)*, Bolton Landing, NY, (pp. 164–177).

Bernstein, D. & Vij, D. (2010). Intercloud security considerations. *2nd IEEE International Conference on Cloud Computing Technology and Science*, (pp. 537–544).

Booch, G., Rumbaugh, J., & Jacobson, I. (1999). *The Unified Modeling Language User Guide.* Reading, MA: Addison Wesley.

Boytsov, A. & Zaslavsky, A. (2011). From sensory data to situation awareness: Enhanced context spaces theory approach. *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)* (pp. 207–214).

Cachin, C. & Schunter, M. (2011, December). A cloud you can trust. *IEEE Spectrum, 48*(12), 28–51.

Case, R. P. & Padegs, A. (1978, January), Architecture of the IBM System/370. *Communications of the ACM, 21*(1), 73–96.

Clausewitz. (1968). *On War.* (J. J. Graham, Trans.). Middlesex, UK: Penguin Books.

Cook, I. P. & Pfleeger, S. L. (2010, May/June). Security decision support: Challenges in data collection and use. *IEEE Security and Privacy, 8*(3), 28–35.

Creasy, R. J. (1981, September). The origin of the VM/370 time sharing system. *IBM Journal of R&D, 25*(5), 483–490.

Daley, R. C. & Dennis, J. B. (1968, May). Virtual memory, processes, and sharing in MULTICS. *Communications of the ACM, 11*(5), 306–312.

Delquié, P. (2008). The value of information and intensity of preference. *Decision Analysis, 5*(3),129–139,169.

Doran, R. W. (1988, October). Amdahl multiple-domain architecture. *Computer*, pp. 20–28.

Endsley, M. R. (1995a). Toward a theory of situation awareness in dynamic systems. *Human Factors, 37*(1), 35-64.

Endsley, M. R. (1995b). Measurement of situation awareness in dynamic systems. *Human Factors, 37*(1), 65–84.

Endsley, M. R. (2000). Direct measurement of situation awareness: Validity and use of SAGAT. In M. R. Endsley & D. J. Garland (Eds.) *Situation Awareness Analysis And Measurement* (pp. 147–174). Mahwah, NJ: Erlbaum.

Fabry, R. S. (1973, November). Dynamic verification of operating system decisions. *Communications of the ACM, 16*(11), 659–668.

Fraser, K., Hand, S., Pratt, I., & Warfield, A. (2004, October). Safe hardware access with the Xen virtual machine monitor. *Proceedings of the 1st Workshop on Operating System and Architectural Support for the on-demand IT Infrastructure*, Boston, MA.

Geer, D. E. & Archer, J. (2012, July/August). Stand your ground. *IEEE Security and Privacy, 10*(4), 96.

Gerken, M., Pavlik, R., Houghton, C., Daly, K., & Jesse, L. (2010). Situation awareness using heterogeneous models. *2010 International Symposium on Collaborative Technologies and Systems (CTS)*, (pp. 563–572).

Giffin, J. (2010, May/June). The next malware battleground: Recovery after unknown infection. *IEEE Security and Privacy, 8*(3), 77–82.

Gifford, D. & Spector, A. (1987, April). Case study: IBM's System 360-370 architecture, *Communications of the ACM, 30*(4), 291–307.

Goldberg, R. P. (1974, June). Survey of virtual machine research. *IEEE Computer, 7*(6), 34–45.

Graaido, J. M., Schlesinger, R., & Hoganson, K. (2013). *Principles of Modern Operating Systems, 2nd Ed.* Burlington, MA: Jones & Bartlett.

Graham, R. & Maynor, D. (2006, January). SCADA security and terrorism: We're not crying wolf. *Blackhat Federal 2006*, Washington, DC.

Guang, T. & Chang, Z. (2011). A framework for the distributed situation awareness (DSA) in C2 of NCW. *2011 International Conference on Intelligence Science and Information Engineering (ISIE)*, (pp. 230–234).

Gum, P. H. (1983). System/370 Extended architecture: facilities for virtual machines. *IBM Journal of Research and Development, 27*(6), 530.

Hole, K. J. & Netland, L. (2010, May/June). Towards risk assessment of large-impact and rare events. *IEEE Security and Privacy, 8*(3), 21–27.

Holsopple, J., Sudit, M., Nusinov, M., Liu, D., Du, H., &Yang, S. (2010, March). Enhancing situation awareness via automated situation assessment. *IEEE Communications Magazine, 48*(3), 146–152.

Jamsa, K. (2013). *Cloud Computing*. Burlington, MA: Jones & Bartlett.

Johnson, M. E. & Pfleger, S. L. (2011, January–February). Addressing information risk in turbulent times. *IEEE Security and Privacy, 9*(1), 49–58.

Jones, R. E. T., Connors, E. S., Endsley, M. R. (2011). A framework for representing agent and human situation awareness, *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, (pp. 226–233).

Kangas, A. (2010). Measuring the value of information in multicriteria decision making. *Forest Science, 26*(6), 558–566.

Kenney, J. R. & Robinson, C. (2010, September/October). Embedded software assurance for configuring secure hardware. *IEEE Security and Privacy, 8*(5), 20–26.

King, S. T., Dunlap, G. W., & Chen, P. M. (2002). Operating system support for virtual machines. *USENIX Technical Conference*.

Krutz, R. L. & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Indianapolis, IN: Wiley Publishing.

Krutz, R. L. & Vines, R. D. (2010). *Cloud security.* Indianapolis, IN: Wiley Publishing.

Lampson, B. W. & Sturgis, H. E. (1976, May). Reflections on an operating system design, *Communications of the ACM, 19*(5), 251–265.

Lan, F., Chunlei, W. & Guoqing, M. (2010). A Framework for network security situation awareness based on knowledge discovery. *2010 2nd International Conference on Computer Engineering and Technology (ICCET)*, Vol. 1, pp. V1-226–V1-231.

Laureano, M., Maziero, C., & Jamhour, E. (2004). Intrusion detection in virtual machine environments. *Proceedings of the 30thEUROMicro Conference (EUROMICRO '04)*.

Lett, A. S. & Konigsford, W.L. (1968). TSS/360: A time-shared operating system. *Proceedings of the Fall Joint Computer Conference*, AFIPS, Vol. 33, part1, pp. 15–28.

Levine, J., Grizzard, J., & Owen, H. (2006, January-February). Detecting and categorizing kernel-level rootkits to aid future detection. *IEEE Security and Privacy Magazine, 4*(1), 24–32.

Liu, Q., Weng, C., Li, M., & Luo, Y. (2010, November/December). An In-VM measuring framework for increasing virtual machine security in clouds. *IEEE Security & Privacy, 8*(6), 56–62.

Lumsden, K. & Mirzabeiki, V. (2008). Determining the value of information for different partners in the supply chain. *International Journal of Physical Distribution & Logistics Management, 38*(9), 659–673.

Lynn, William J. III, (2010, September/October). Defending a new domain: The Pentagon's cyberstrategy, *Foreign Affairs*.

Ma, J. & Zhang, G. (2008). Team situation awareness measurement using group aggregation and implication operators. *3rd International Conference on Intelligent System and Knowledge Engineering, ISKE 2008,* Vol. 1, pp. 625–630.

Meyer, R.A. & Seawright, L.H. (1970). A virtual machine time-sharing system. *IBM Systems Journal, 9*(3), pp. 199–218.

Mihailovic, A., Chochliouros, I. P., Georgiadou, E., Spiliopoulou, A. S., Sfakianakis, E., Belesioti, M., Nguengang, G., Borgel, J., & Alonistioti, N. (2009). Situation awareness mechanisms for cognitive networks. *International Conference on Ultra Modern Telecommunications & Workshops, ICUMT '09*, pp. 1–6.

Naraine, R. (2006). 'Blue Pill' prototype creates 100% undetectable malware, *eWeek.com*, http://www.eweek.com/article2/0,1895,1983037,00.asp

Nwiabu, N., Allison, I., Holt, P., Lowit, P., & Oyeneyin, B. (2011). Situation awareness in context-aware case-based decision support, *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 9–16.

Oppenheim, C. et.al. (2003a). Studies on information as an asset 1: definitions, *Journal of Information Science, 29*(3), 159–166.

Oppenheim, C. et.al. (2003b). Studies on information as an asset 2: repertory grid, *Journal of Information Science, 29*(5), 419–432.

Oppenheim, C. et.al. (2003c). Studies on information as an asset 3: views of information professionals, *Journal of Information Science, 30*(2), 181–190.

Osinga, F. (2005). *Science strategy and war: The strategic theory of John Boyd.* Abingdon, UK: Routledge.

Parvar, H., Fesharaki, M. N. & Moshiri, B. (2010). Shared situation awareness system architecture for network centric environment decision making. *2010 Second International Conference on Computer and Network Technology (ICCNT),* pp. 372–376.

Peterson, J. L., Silberschatz, A., & Gagne, G. (1983-2004). *Operating System Concepts*. (Eds.1-7). Hoboken, NJ: John Wiley & Sons.

Popek, G. J. & Goldberg, R. P. (1974, July). Formal requirements for virtualizable third generation architectures. *Communications of the ACM, 17*(7), 412–421.

Popek, G. A. & Farber, D. A. (1978, September). A model for verification of data security in operating systems. *Communications of the ACM, 21*(9), 737–749.

Rahman, M. (2011) Somatic situation awareness: a model for SA acquisition under imminent threat and severe time stress. *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 257–263.

Rutkowska, J. (2005, March). Rootkits stealth by design malware. Amsterdam: *BlackHat Europe*.

Schiffman, J., Moyer, T., Jaeger, T., & McDaniel, P. (2011, January–February). Network-Based root of trust for installation. *IEEE Security and Privacy, 9*(1), 40–48.

Seawright, L. H. & McKinnon, R. A. (1979). VM/370 – A study of multiplicity and usefulness. *IBM Systems Journal, 18*(1), 4–17.

Shapiro, J. S., Vanderburgh, J., Northrup, E., & Chizmadia, D. (2004). Design of the EROS trusted window system. *Proceedings of the 13th USENIX Security Symposium*, pp. 165–178.

Shepanski, A. (1984). The value of information in decision making. *Journal of Economic Psychology, 5*(2), 177–194.

Skoudis, E. & Zeltser, L. (2003). *Malware: Fighting malicious code.* Upper Saddle River, NJ: Prentice Hall.

St. John, M. & Smallman, H. S. (2008). Staying up to speed: Four design principles for maintaining and recovering situation awareness. *Journal of Cognitive Engineering and Decision Making, 2*, 118–139.

Stone-Gross, B., Cova, M., Gilbert, B., Kemmerer, R., Kruegel, C., & Vigna, G. (2011, January-February). Analysis of a botnet takeover. *IEEE Security and Privacy, 9*(1), 64–72.

Stanton, N. A., Salmon, P. M., Walker, G. H., & Jenkins, D. P. (2010). Is situation awareness all in the mind?. *Theoretical Issues in Ergonomics Science, 11*(1–2), 29–40.

Stytz, M. R. & Banks, S. B. (2006, June). Metrics for assessing command, control, and communications capabilities. *11th International Command and Control Research and Technology Symposium,* San Diego, CA.

Stytz, M. R. & Banks, S. B. (2006, April). Metrics to assess command, control, and communications (C3) performance within a network-centric warfare simulation. *Proceedings of the SPIE Conference on Enabling Technologies for Simulation Science X, 6227*, CD-ROM.

Stytz, M. R. & Banks, S. B. (2004, April). Toward computer generated actors as cyber space opposing forces used in network centric warfare simulations. *Proceedings of the 2004 Spring Simulation Interoperability Workshop*, Washington, DC; pp. 84–95.

Takabi, H., Joshi, J. B. D., & Ahn, G. (2010, November/December). Security and privacy challenges in cloud computing environments. *IEEE Security & Privacy, 8*(6), 24–31.

Uhlig, R., Neiger, G., Rodgers, D., Santoni, A. L., Martins, F. C. M., Anderson, A.V., Bennett, S. M., Kagi, A., Leung, F. H. & Smith, L. (2005, May). Intel virtualization technology, *IEEE Computer, 38*(5), 48–56.

Vachon, F., Lafond, D., Vallières, B.R., Rousseau, R., & Tremblay, S. (2011). Supporting situation awareness: A tradeoff between benefits and overhead. *IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 284–291.

Xi, R., Jin, S., Yun, X., & Zhang, Y. (2011). CNSSA: A comprehensive network security situation awareness system. *IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 482–487.

AUTHORS

Martin R. Stytz (mstytz@att.net, mstytz@gmail.com) is a professor at the University of Maryland University College and a research professor at Georgetown University. He received a BS from the U.S. Air Force Academy in 1975, an MA from Central Missouri State University in 1979, an MS from the University of Michigan in 1983, and his PhD in computer science and engineering from the University of Michigan in 1989. His research interests span the fields of computer science, human behavior and intelligence, and medicine. Specific current interests include virtual environments, distributed interactive simulation, distributed systems, modeling and simulation, large-scale system architecture, design, & development, cyberwarfare, distributed simulation, distributed virtual environments, user-centered decision support, intelligent agents, information security, cyber security, and software engineering.

Sheila B. Banks (sbanks@calculated-insight.com) is the president of Calculated Insight and a professor at the University of Maryland University College. Banks received her BS from the University of Miami, Coral Gables, Florida, in 1984 and a BS in electrical engineering from North Carolina State University, Raleigh in 1986. Also from NCSU, Raleigh she received an MS in electrical and computer engineering in 1987 and her PhD in computer engineering (artificial intelligence) from Clemson University, Clemson, South Carolina, in 1995. Her research interests include artificial intelligence, human behavior and cognitive modeling, intelligent computer generated forces, associate and collaborative systems, distributed virtual environments, intelligent human computer interaction, and man-machine interfaces.

Multidisciplinary Approaches for Cyber Security

J. Todd McDonald, PhD | Lee M. Hively, PhD

ABSTRACT

Today's cyberspace is a powerful, virtual environment enabled by a pervasive global digital infrastructure. Even though it offers an ideal landscape for the conduct of commerce, science, education, communication, and government, cyberspace remains vulnerable to attack and manipulation from ever-evolving malicious threats. Cyber security, like other research disciplines, must often draw upon disparate fields of study in order to advance and create applied security measures that ensure adequate levels of confidentiality, integrity, and authentication. In this paper, we use a real world example to illustrate an applied multidisciplinary approach and argue that holistic and collaborative efforts foster the best environment for advancing the field of cyber security.

INTRODUCTION

Researchers often face challenging problems in the engineering and science fields that are only solved through years of continual experimentation and effort that result in small, incremental steps forward in progress. Engineers and scientists are typically experts in their fields of study and do not have time to remain current on the advances made in other disparate fields. Sometimes research problems are uniquely addressed only by applying theoretical and practical results from different scientific areas of study. The pervasiveness of the cyber domain in almost every aspect of modern life—from government to private sector—has brought the issue of security research squarely to the forefront of international attention. As such, the need for multidisciplinary approaches to help solve the hard problems of security has become paramount as well.

The impact of malicious cyber attacks on various commercial enterprises and military systems can now reach catastrophic proportions in terms of financial loss and compromise of critical information. Lockheed Martin, RSA, Google, Citigroup, the International Monetary Fund, MasterCard, the U.S. Chamber of Commerce, and the U.S. Department of Defense have all reported breech and infiltration through hackers in the last two years (Johnson, 2011; Shachtman, 2011; Wyler, 2011; Thomas & Katrandjian, 2011; Hack Against Citigroup, 2011). In 2011, 70 million Sony PlayStation users had their credit card information compromised (Johnson, 2011). In 2009, the worldwide ATM Industry Association reported over $1 billion in annual global losses from credit card fraud and electronic

crime associated with ATMs (Siciliano, 2009). In 2011, the Federal Bureau of Investigation's Internet Crime Complaint Center (IC3) reported that it had received 314,246 complaints with a reported dollar loss of $485.3 million (Internet Crime Report, n.d.). Finally, Richard Clarke, the former U.S. government security chief that prognosticated the 9/11 attacks on the U.S., asserted recently (Waugh, 2012) that every major company in the U.S. has already been penetrated by Chinese hackers looking to steal military and financial secrets.

The state of the art for security research and realized security solutions is often outpaced by the sophistication and number of attacks carried out by nation-state and organized cyber-criminals. In cyber security, we can look historically to see how the marriage of multiple disciplines has allowed novel insight in the advancement of both theoretical results and practical applications. In 1882, a telegraph engineer named Frank Miller first described the concept of a one-time pad (OTP) data cipher (Miller, 1882), where ciphertext is created by modular addition of plaintext and key material of equal length. In 1918, AT&T Bell Labs engineer Gilbert Vernam used the same concept to patent an automated telegraphic switching system where the XOR combining function was implemented through relay switches (Vernam, 1926). In 1948, computer scientist Claude Shannon pioneered the field of information theory based on his wartime research of cryptographic algorithms (Shannon, 1948). He proved that the one-time pad implementation was information-theoretically secure by virtue that the entropy between the plaintext and ciphertext was maximal based on mutual information probabilities (Shannon, 1949). In essence, OTP is unbreakable even given unlimited computational power. However, the one-time pad has the limitation that the key size must be equal to the plaintext size.

Given the fact that the one-time pad is a symmetric key algorithm, the transmission of the key between parties is extremely problematic and not practical for common applications. It was not until the last decade that this limitation could be overcome based on breakthroughs in the area of quantum physics. Quantum Key Distribution (Mink, Tang, Ma, Nakassis et. al., 2006), for example, has been realized in physical systems and allows the transmission of large key bits. Unconditional security of quantum key generation protocols derives from quantum laws, Heisenberg's uncertainty principle, and the fact that quantum information cannot be copied or measured without detection. Quantum cryptography is in the advanced experimental and developmental stage, and well on its way to full commercial realization in the next decade.

Ultimately, a major problem of cyber security (confidentiality in this example) has been advanced through a series of combined work and novel contributions in multiple disparate disciplines. We believe other cyber security areas can and will be furthered in a similar manner. We illustrate next our experience with developing accurate and fast methods for cyber anomaly detection and demonstrate the concept of multi-disciplinary synergy.

REAL WORLD CONTEXT: EVENT FOREWARNING AND DETECTION

Forewarning and detection of anomalous events in the cyber domain has massive implications for improved operational readiness and ensuring security of mission-critical systems. Unfortunately, forewarning and detection are only useful if they are reliably actionable. Although high true positive rates can be achieved for various methods of anomaly detection using a wide variety of data correlation, high false positive rates cause a loss of confidence in applied tools and reduced efficiency for operational communities in both the government and commercial sectors. We are currently advancing a novel approach for cyber event forewarning and detection based upon side-channel power information. Our methodology uses a theorem-based, data-driven analysis technique (Hively& Protopopescu, 2003) with over a decade of historic success for fast and accurate forewarning in physiological and industrial domains (Protopopescu & Hively, 2005; Bubacz, Chmielewski, Depersio, Pape, Hively, Abercrombie, & Boone, 2011; Protopopescu & Hively, 2003; Hively, Protopopescu, Maghraloui, & Spencer, 2001; Hively & Clapp, 1996; Hively& Protopopescu, 2004; Hively, 2011).

The foundation for our work is based on phase space dissimilarity measures (PSDM) that have been used to successfully forewarn of epileptic seizure events from scalp brain waves (Hively, Protopopescu, & Munro, 2005, Gailey, Hively, & Protopopescu, 1999; Hively, Gailey, & Protopopescu, 1999). Figure 1 depicts EEG data, e, that are sampled at equal time intervals,τ, starting at an initial time, t_0, yielding a time-serial set of N points (cutset), $e_i = e(t_0 + i\tau)$. Artifacts (eyeblinks and other muscular activity) are then removed with a zero-phase quadratic filter that fits a parabola in the least-squares sense over a moving window of $2w+1$ data points. The central point of the fit estimates the low-frequency artifact, f_i. The residual (artifact-filtered) signal, $g_i = e_i - f_i$, has essentially no low-frequency artifact. The g_i-data are symbolized into S discrete values, s_i, namely $0 \le s_i \le S - 1$. Uniform symbols, $s_i = \mathrm{INT}[S\,(g_i - g_n)/(g_x - g_n)]$, have use g_x and g_n, which are the maximum and minimum in the g_i-data, respectively.

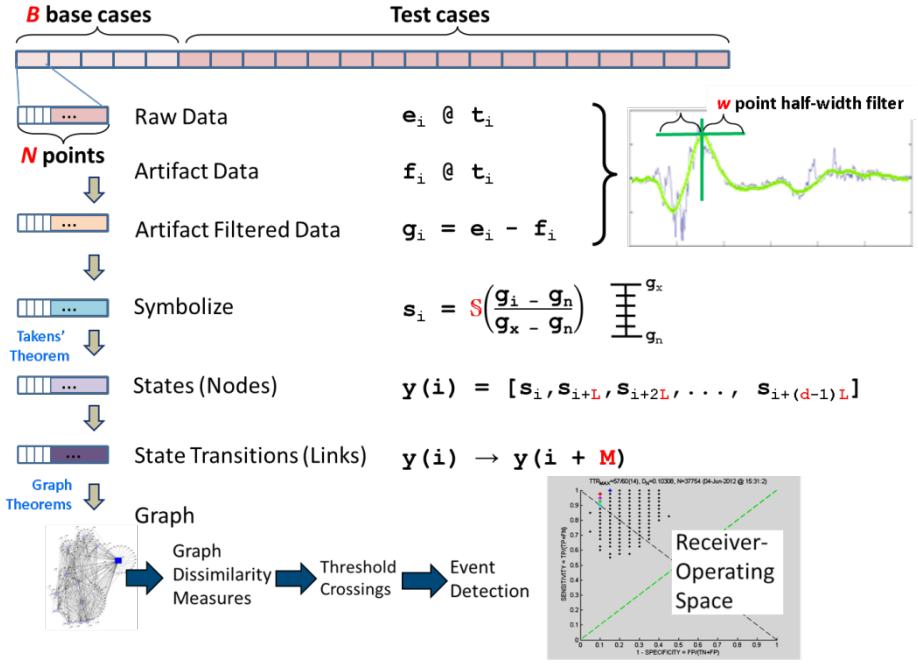

FIGURE 1: PHASE SPACE CREATION FROM TIME SERIAL EEG DATA.

The first provable component uses Takens theorem (Takens, 1981) to construct time-delay-embedding states via the vector, $y(i) = [s_i, s_{i+L}, \ldots, s_{i+(d-1)L}]$. The dynamical states are nodes, and the state-to-state transitions are links, $y(i) \to y(i + M)$, in a mathematical graph. Graph theorems (Diestal, 2005) guarantee graph-invariant measures. Dissimilarity measures are differences in these graph-theoretic measures for two cutsets. Normalized measures, $U_i(V) = |V_i - \bar{V}|/\sigma$, account for the disparate range and variability of the dissimilarities. The mean dissimilarity measure, $\bar{V}$, is obtained by comparison among the $B(B-1)/2$ unique combinations of the B base case segments, with a corresponding sample standard deviation, σ. Each contiguous, non-overlapping test case is subsequently compared to each of the B base case intervals to obtain the corresponding average dissimilarity, V_i, of the i-th analysis window for each dissimilarity measure. U_i is then the number of standard deviations that the i-th test case (unknown

dynamics) deviates from the base case (nominal-state). Several successive occurrences of U_i above a threshold provide indication of an event forewarning. The measures of success are the number of true positives (TP) from known events (Ev = 40) datasets, and the number of true negatives (TN) from known non-events (NEv = 20) datasets. We determine the best parameter values in the set, {d, S, L, M, w, B, N} by minimizing minimum prediction distance, which has the form: $D = \{[1 - (TP/Ev)]^2 + [1 - (TN/NEv)^2\}^{1/2}$. Equivalently, false negatives are no indication of an event, and false positives are forewarning for a non-event.

Figure 2 illustrates the forewarning analysis which trains the hyper-dimensional parameter search space and produces a receiver-operating space. A specific parameter set produces a collective assessment of true positives and false positives for the 60 data sets, given knowledge of whether an event (seizure) took place. Using PSDM, we have achieved prediction distances (seen in figure 2 as the distance from perfect forewarning) in the range of 0.09 – 0.15 and have achieved a forewarning accuracy of 58/60 with sensitivity (true positive rate) of 40/40 and specificity (true negative rate) of 18/20. The probability of this forewarning occurring by chance in the receiver-operating space is $< 2 \times 10^{-10}$.

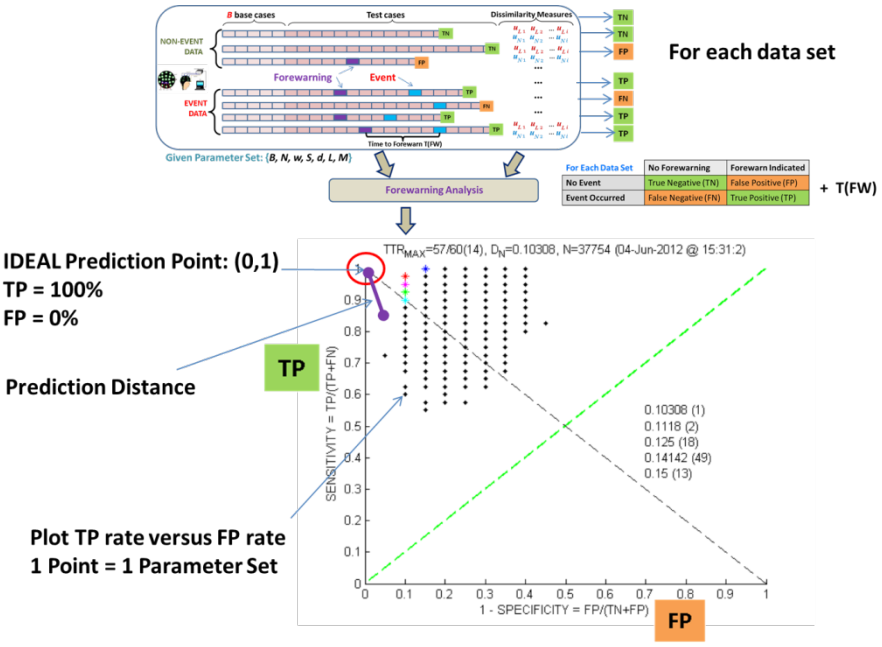

FIGURE 2: PHASE SPACE DISSIMILARITY ANALYSIS AND FOREWARNING PREDICTION.

In summary, Takens' theorem allows conversion of time-serial observations to time delay embedding states. This diffeomorphism provides states (nodes) and state-to-state transitions (links) that provide connectivity and directivity in the resultant graph. Graph theorems guarantee that the graph-invariant measures can capture topological invariants.

Consequently, this approach is a data-driven model of dynamical change, thus allowing event forewarning. EEG analysis and epileptic seizure prediction (a biomedical application) represents only one successful application of this approach. Equipment demonstrations include damage progression in a full-size bridge from accelerometer data (Bubacz,

Chmielewski, Depersio, Pape, Hively, Abercrombie, & Boone, 2011) and failure forewarning in motors and motor-driven components from accelerometer and electrical data (Protopopescu & Hively, 2005). Other biomedical demonstrations include use of chest heart waves to forewarn of heart attacks, fainting, and septic shock, and the detection of breathing difficulty from chest sounds (Protopopescu & Hively, 2005). The last application received an R&D100 Award from *R&D Magazine* in 2005, and involves wireless data exchange and analysis on a hand-held device.

COMBINING DISCIPLINES FOR NOVEL CYBER SECURITY ADVANCEMENT

Our experience with event forewarning and detection illustrates the synergy and usefulness of leveraging results from disparate scientific fields of study. Electrical engineering and physics has advanced the thought of time-series data analysis to provide novel insight into non-linear dynamics and how dynamical systems work. Abstract mathematics has a rich history in framing the theoretical statements about graphs and their properties. Industrial and civil engineers have laid solid foundations for how to predict failures and cracks in material properties. Medical research has framed the study of various physical ailments so that we can relate physical observations to manifestations of biomedical events such as seizures and heart attacks. Statistics gives us a framework to assign confidence to predictive estimates and determine whether predictions are better than guessing. Computer science gives the computational tools for analysis of real data. Our PSDM approach is a result of advancements in all of these combined fields and the technique would not be robust without the synergistic contributions of all of them.

To further cyber security, we are now experimenting with PSDM to determine its efficacy for cyber anomaly detection. Recently, computers have been modeled using nonlinear dynamics-based measurement frameworks (Mytkowicz, Diwan, & Bradley, 2009; Alexander, Mytkowicz, Diwan, & Bradley, 2010). Appealing to a physics-based view of the system, results indicate that the dynamics of a computer can be described by an iterated map representing the software and hardware. Based upon time-series data from simple programs running on common computers, researchers have similarly used Taken's delay-coordinate embedding (Takens, 1981) to study the associated dynamics. As a result, researchers have found strong indications of a low-dimensional attractor in the dynamics of simple programs as well as showing the first experimental evidence of chaos in real computer hardware (Mytkowicz, Diwan, & Bradley, 2009).

Side-channel information (particularly differential power analysis) has been used extensively for adversarial compromise of algorithms and has allowed exploitation of cryptographic operations implemented in hardware (Kocher, Jaffe, & Jun, 1998; Kocher, Jaffe, & Jun, 1999; Mangard, Oswald, & Popp, 2007). As a natural extension to this approach, our vision is to use side-channel power information sampled from various computer components (external aggregate AC power, internal aggregate DC power, motherboard, CPU, disk drive, memory, network interface cards, and graphics cards) to characterize normal operational behavior in cyber systems. Based upon side-channel characterization from non-invasive sensors, we will apply PSDM to evaluate forewarning and detection possibilities for cyber related scenarios. Of interest to cyber security, we are interested in whether the execution of anomalous software can be detected. We define three broad classifications for systems under study based on increasing complexity for characterizing their baseline activity at the side-channel level: 1) SCADA/industrial control systems; 2) high performance and cluster computing; and 3) enterprise desktops.

Accurate and fast cyber anomaly detection, particularly for malicious software execution, would considerably bolster the security of organizations in a plethora of communities: industry, commerce, military, academia, and the everyday user. As we and other researchers press forward with possible solutions, we believe that leveraging multi-disciplinary theories and applied research is the ideal pathway. We also believe that other areas of cyber security would benefit from this collaborative approach.

INCREASED OPPORTUNITIES

A collaborative research method for cyber security also introduces numerous coincidental benefits. Students from a wide range of studies (math, biology, engineering, computer science, medicine, etc.) are needed for their strengths in specific areas. University collaboration is fostered because schools with strong research areas in specific fields provide possibility for joint research. Synergistic research can also tap into the capabilities of national laboratories, which typically have the brightest and best researchers in a particular focus area. In addition to the benefits of leveraging the respective strengths of student, faculty, and laboratory researchers, multidisciplinary approaches for cyber security eventually result in tangible artifacts. For example, there are increased possibilities for patents and copyrights, as well as technology transfer. Scholarly publication and the advancement of knowledge are also key benefits when researchers look outside their own field of expertise as they pursue their research goals.

CONCLUSIONS

The nature of good research can be characterized by asking good questions that are relevant to current hard problems. We illustrate in this paper how advancement in one area may be enhanced and predicated by the theoretical advancements in disparate fields, opening up collaborative opportunities with researchers, students, and practitioners from diverse communities. We argue that cyber security, as a research field, will continue to benefit from outside-the-box thinking in order to develop and implement novel solutions to the problems facing the computer world. As we have pursued the applicability of phase space dissimilarity analysis to the cyber anomaly detection problem, we have observed that incorporation of research from non-linear dynamics, physics, graph theory, electrical engineering, computer engineering, and statistics is creating a new set of research questions, which will frame work for years to come.

ACKNOWLEDGMENTS

This research was supported in part by an appointment to the U.S. Department of Energy (DOE) Higher Education Research Experiences (HERE) for Faculty at the Oak Ridge National Laboratory (ORNL) administered by the Oak Ridge Institute for Science and Education.

REFERENCES

Alexander, Z., Mytkowicz, T., Diwan, A., & Bradley, E. (2010). Measurement and dynamical analysis of computer performance data. *IDA 2010,*18-29.

Bubacz, J. A., Chmielewski, H. T., Depersio, A. J., Pape, A. E., Hively, L. M., Abercrombie, R. K. & Boone, S. D. (2011, August). Phase space dissimilarity Measures for structural health monitoring. *ORNL/TM-2011/260.* Oak Ridge National Laboratory.

Diestel, R. (2005). *Graph Theory*, 3rd ed. Heidelberg: Springer-Verlag.

Gailey, P. C., Hively, L. M., & Protopopescu, V. A. (1999, June 28–July 1). "Robust Detection of Dynamical Change in EEG," *Proceedings of 5th Experimental Chaos Conference,* Orlando, Florida.

Hack against Citigroup Revealed – Is Bank Security System Really Bullet-Proof? (2011, June 9). *International Business Times New York.* Retrieved from http://newyork.ibtimes.com/articles/160322/20110609/citibank-hacked-security-online.htm.

Hively, L. M. (2011, October 6). Graph-theoretic analysis of discrete-phase-space states for condition change detection and quantification of information. *Preliminary patent application #61543950* to USPTO.

Hively, L. M. & Clapp, N. E. (1996, March). Nonlinear analysis of polygraph data. *K/NSP-351.* Oak Ridge National Laboratory, Oak Ridge, TN.

Hively, L. M., Gailey, P. C., Protopopescu, V. A. (1999, March). "Sensitive Measures of Condition Change in EEG Data," *Proceedings of International Workshop Chaos in Brain.* Bonn: World Scientific.

Hively, L. M., Gailey, P. C., & Protopopescu, V. A. (1999). Detecting dynamical change in nonlinear time series. *Physics Letters.* A 258:103-114W.

Hively, L. M. & Protopopescu, V. A. (2004, June). Machine failure forewarning via phase-space dissimilarity measures. *Chaos 14,*408-419.

Hively, L. M. & Protopopescu, V. A. (2003, April 6–11). Detection of changing dynamics in physiological time series. *Proceedings of ANS Conference on Nuclear Mathematics Computational Sci.* Gatlinburg, TN.

Hively, L. M., Protopopescu, V. A., Maghraloui, M. & Spencer, J. W. (2001, November). Annual Report for NERI Proposal #20000109 on Forewarning of Failure in Critical Equipment at Next-Generation Nuclear Power Plants. *ORNL/TM-2001/195.*

Hively, L. M., Protopopescu, V. A., & Munro, N. B. (2005, December). Enhancements in epileptic forewarning via phase space dissimilarity. *Journal of Clinical Neurophysiology. 22,* 402-409.

Internet Crime Report. U.S. Federal Bureau of Investigation, Internet Crime Complaint Center. Online: http://www.ic3.gov/media/annualreports.aspx/.

Johnson, R. (2011, June 13). The biggest hacking attacks of 2011. *Business Inside*. Online: http://www.businessinsider.com/imf-cyber-attacked-hackers-sony-rsa-lockheed-martin-epsilon-michaels-2011-6?op=1

Kocher, P., Jaffe, J., & Jun, B. (1999). Differential power analysis. *Proceeding of the 19th Annual International Cryptology Conference on Advances in Cryptology (CRYPTO '99)* (pp. 388–397). Heidelberg: Springer-Verlag.

Kocher, P., Jaffe, J., & Jun, B. (1998). Introduction to differential power analysis and related attacks. *Technical Report*, Cryptography Research Inc.

Mangard, S., Oswald, E., & Popp, T. (2007). Power analysis attacks: Revealing the secrets of smart cards. *Advances in Information Security.* Heidelberg: Springer-Verlag.

Miller, F. (1882). *Telegraphic code to insure privacy and secrecy in the transmission of telegrams*. New York: Charles M. Cornwell.

Mink, A., Tang, X., Ma, L., Nakassis, T. et al. (2006). High Speed Quantum Key Distribution System Supports One-Time Pad Encryption of Real-Time Video. In E. J. Donker, A. R. Pirich, & H. E. Brandt (Eds.) *Proceedings of SPIE Quantum Information and Computation IV* pp. 6244: 62440.

Mytkowicz, T., Diwan, A., & Bradley, E. (2009). Computer systems are dynamical systems. *Chaos 19,* 033124.

Protopopescu, V. & Hively, L. M. (2005). Phase-space dissimilarity measures of nonlinear dynamics: Industrial and biomedical applications. *Recent Research Developments in Physics, 6,* 649-688.

Protopopescu, V. A., & Hively, L. M. (2003, June). Forewarning of machine failure via nonlinear analysis. *Proceedings of the American Nuclear Society*.

Shachtman, N. (2011, October 7). Computer virus hits U.S. drone fleet. *Wired*. Online: http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/

Shannon, C. (1948, July & October). A mathematical theory of communications. *Bell System Technical Journal, 27*, 379–423 & 623–656.

Shannon, C. (1949). Communication theory of secrecy systems. *Bell System Technical Journal,* 28(4), 656–715.

Siciliano, R. (2009, April 7). Credit card fraud tops consumers concerns. *Finextra*. Online: http://www.finextra.com/community/fullblog.aspx?id=2756.

Takens, F. (1981). Detecting strange attractors in turbulence. In D. A. Rand & L.S. Young(Eds.), *Dynamical systems and turbulence, lecture notes in mathematics* (pp. 366–381), Heidelberg: Springer-Verlag.

Thomas, P. & Katrandjian, O. (2011, December 21). Chinese hack into US chamber of commerce, authorities say. *ABC News*. Online: http://abcnews.go.com/International/chinese-hack-us-chamber-commerce-authorities/story?id=15207642.

Vernam, G. (1926). Cipher printing telegraph systems for secret wire and radio telegraphic communications. *Journal of the IEEE, 55*, 109–115.

Waugh, R. (2012, March 28). Cyber-espionage warning from U.S security chief who warned of 9/11. *Daily Mail Online*. Online: http://www.dailymail.co.uk/sciencetech/article-2121624/Every-major-company-U-S-hacked-China-Cyber-espionage-warning-U-S-security-chief-warned-9-11.html.

Wyler, G. (2011, June 13). Pentagon admits 24,000 files were hacked, declares cyberspace a theater of war. *Business Insider.* Online: http://articles.businessinsider.com/2011-07-14/politics/30034321_1_cyber-threat-cyber-attacks-new-command.

AUTHORS

J. Todd McDonald (jtmcdonald@southalabama.edu) is a professor of computer science in the School of Computing at the University of South Alabama. McDonald received his PhD in computer science from Florida State University in 2006, his MS in computer engineering from the Air Force Institute of Technology in 2000, and his BS in computer science from the U.S. Air Force Academy in 1990. His research interests include program protection and exploitation, secure software engineering, and information assurance; he served over 20 years in the U.S. Air Force as a cyber operation officer and is a retired lieutenant colonel. McDonald has published over 30 refereed papers and journals in the area of cyber security and has shared in over $5 million of grant funding from the National Science Foundation, Air Force Office of Scientific Research, and the Air Force Research Laboratory.

Lee M. Hively (lee.m.hively@hughes.net) did this work as a senior cybersecurity researcher in the Cyber Information and Security Research Group at Oak Ridge National Laboratory. Hively received bachelor's degrees in engineering science, mathematics, general arts and sciences (1970, Pennsylvania State University); an MS in physics (1971, University of Illinois, Urbana); and a PhD in nuclear engineering (1980, University of Illinois, Urbana). His research includes millimeter waveguides and general relativity (1970–1974) at the Western Electric Company's Engineering Research Center, Princeton, New Jersey; controlled fusion plasmas, nonlinear and graph-theoretic analysis of time-serial data, and more-complete electrodynamics at Oak Ridge National Laboratory, Oak Ridge, Tennessee (1984–2014). He has mentored many high school, undergraduate, and graduate students, publishing over 150 peer-reviewed papers, including 13 patents and 2 patents pending.

Geospatial Mapping of Internet Protocol Addresses for Real-Time Cyber Domain Visual Analytics and Knowledge Management Using the Global Information Network Architecture

Thomas Anderson, PhD | Curtis L. Blais | Don Brutzman | Scott A. McKenzie

ABSTRACT

The development of new capabilities in the cyber security domain is necessary to meet and defeat the persistent cyber-attacks that threaten national security. Too much data is generated from network behavior pertaining to normalcy, failure, and hostile attacks. The network analyst cannot effectively and efficiently monitor, recognize, and respond to cyber-attacks. Putting any amount of effort into a particular, singular stove-piped solution is too costly in time and money and does not keep pace with the network threats. We implement a configured specification for real-time cyber domain visual analytics and knowledge management in the Global Information Network Architecture (GINA). GINA provides an environment for defining and integrating data semantics and processing logic to enable rapid development of software applications comprised of new and existing systems through configuration. We construct an application for mapping geospatial locations of participants in the Naval Postgraduate School's Massively Multi-player Online War Game Leveraging the Internet (MMOWGLI) in an analysis program: the Asymmetric Threat Response and Analysis Program (ATRAP). Through the GINA model, there is ready access to participant location and reporting to assist in evaluations. This demonstration of GINA for the geospatial understanding of network entities indicates that it is a viable way forward for a System of Systems (SoS) solution with a configurable component topology in the cyber domain.

Keywords: visualization, cyber, attack, network, SoS, MMOWGLI, ATRAP, GINA, analyst, location, configurable, information, model

INTRODUCTION

As systems and information become more readily network accessible, expert systems become larger, more ambitious, and ultimately must meet expectations that new capabilities immediately set in the realm of the possible. The plethora of independent capabilities or resources in any domain must be aggregated for greater capability. Ultimately the critical attributes that a System of Systems (SoS) must contend with are evolving standards, legacy system(s) capability, and the rapid emergence of new technologies. The state of the art approach for developing systems is with Service Oriented Architecture (SOA) or middleware. Every attempt at a large heterogeneous SoS solution has met the inevitable fate of failure and cancellation due to cost overruns attributed to the geometric explosion of system complexity associated with attempted re-wiring of SOA's brittle system component topography to keep pace with rapidly evolving technology components and sub systems. Prime examples of such failure are Air Force Enterprise Resource Planning (Kanaracus, 2012), Secure Border Initiative-network (CNN, 2011), and Obamacare (Scott, 2013).

Cyber represents a relatively new domain that has many of the attributes that lend itself to an SoS approach when developing capabilities that aggregate or extend new and existing capabilities or data: evolving standards, diverse legacy system(s) capabilities, and the rapid emergence of new technologies driven by an adaptive and evolving threat space. To embark on a cyber domain solution we reflect on the past 20 years of SOA failure and adopt a model-based approach that adheres to the premise that it is better to design and configure a model of the system than it is to write and compile code. Coding is unreliable, error-prone, and brittle, whereas a model is more effective at capturing semantics while dramatically reducing the need for code. The model is configured and thus inherently non-brittle and reconfigurable.

OVERVIEW/CONCEPTUAL FRAMEWORK

Visual Analytics

Visual Analytics provides a means to visually explore massive amounts of data to enable geographic and temporal cognitive understanding of datasets featuring geospatial and temporal components. It is an inherently integrated approach combining visualization, human factors, and data analysis (Keim et. al., 2006); it combines the computers' capabilities for computational information management of big data and complex algorithmic process with the human ability to visually detect patterns or anomalies. Visual analysis enables the intuitive representation of textual and numerical information where pattern recognition, trends, and relationships may be cognitively discerned by humans more easily than by computational methods alone (Hidalgo, 2010).

A subdomain of Visual Analytics is geospatial visual analytics: realizing information and information's associated locations and times — a context that humans inherently understand in terms of geo-political boundaries, geo-locations and events that are also associated with global threats, as well as local and regional phenomena (Boulos et al., 2011; Guo, 2007). For this Cyber use case, it is a means to enhance cognitive decision-making associated with identifying security vulnerabilities relating to unauthorized access to game information from global regions known for malicious attacks, or cyber espionage. Internet Protocol (IP) address to geographic location mapping is a capability that has been around for several years (Hicks, 2013). It is acknowledged that determining the geographic location of game participants based on their IP addresses is not as fool-proof as a fully "grounded cyberspace" (Denning & MacDoran, 1996) would be, since source and intermediate IP addresses can vary significantly for users. However, for this prototype Global Information Systems (GIS) visual analytic application, it will suffice to illustrate the system concept.

We present a system of systems (SoS) approach to near-real time geospatial visual analytics in the cyber domain and describe the implementation of this approach as a model configured in the Global Information Network Architecture (GINA). Our use case model is comprised of the Naval Postgraduate School's online war game (MMOWGLI), the Army's visual geo-spatial event-based Asymmetric Threat Response Analysis Program (ATRAP) (The University of Arizona & Ephibian, Inc., 2011), and an IP address GIS reference database. We construct an application for examining and visualizing locations of MMOWGLI users in ATRAP. A hypergraph of this system with abstracted component system data represented as {Xi} in Figure 1. Each component exists and operates as it was originally designed, but is now functioning as an interoperable capability in the larger SoS that the GINA model specifies. Further, the system model may be readily reconfigured to address different data sources, data visualizations, analytic capabilities, or behaviors.

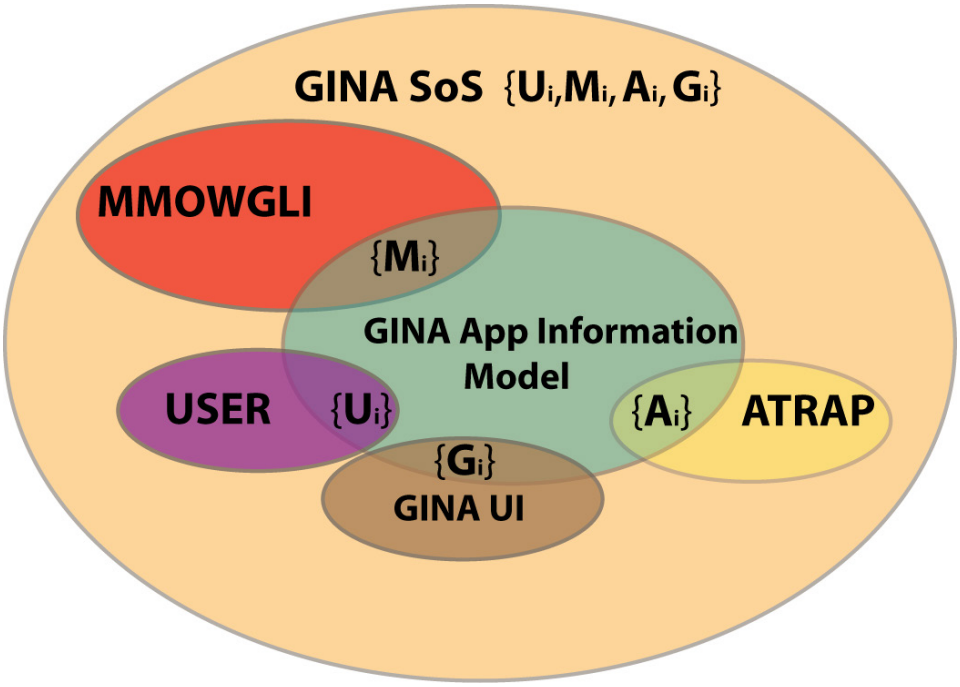

FIGURE 1. HYPERGRAPH SHOWING SYSTEM COMPONENTS AND INTEGRATION OF INFORMATION. THE GINA ENVIRONMENT HAS THE USER AS A COMPONENT IN THE SOS MODEL.

The Global Information Network Architecture (GINA)

Middleware comes from the traditional viewpoint that interoperability is a process of getting systems to talk to each other — an approach that has been proven to be code-intensive, brittle, and subject to a geometric Complexity Curve (cost and time intensive). GINA takes an entirely new approach: model the interoperation as a semantically-rigorous, executable description of domain-relevant, interconnected information objects, and then map the semantics of the resulting information objects to the unique semantics and syntax of the underlying systems. The resulting models are well described, extensible, and robust.

GINA provides full syntactic, semantic, ontological, and operational interoperability without the need for middleware. It provides a System of Systems capability, meaning that within the GINA environment separate systems function as though they were components of a single system, i.e., each system communicates and interoperates with other systems as if they are part of the same model, no matter how disparate and disconnected they are. (Interoperation is a more robust capability as compared to interaction.) Each individual data element is interoperable and usable by any component system within the system of systems.

GINA is a patented network resident environment developed at the Naval Postgraduate School providing a coherent, universally configurable, and extensible model that allows the specification and use of information resources within and across all domains. As a platform for data collection and analysis, GINA provides an environment for defining and integrating data semantics and processing logic to enable rapid development of software applications. GINA provides complete facilities for managing information and services available on accessible networks. It can aggregate and objectify information from an unlimited set of heterogeneous information sources or service providers into a common information model that can be tailored to

specific system behaviors based on the relationship of the user to the information. A well-documented use case and GINA model implementation is an analysis of alternatives capability for Directed Energy Weapons (NPS SE Team Bravo, Cohort 19, 2013) that was developed and configured by a single Navy Lieutenant. Other example applications include the Dragon Pulse command and control (C2) system, the interactive Common Operational Picture (iCOP), and the Consumer Devices Information Management System for reporting Improvisational Exploding Devices (IEDs) for actionable information (Dolk et al., 2012).

Through the model specification, the information objects and services can be referenced, transformed, combined, and/or repurposed in any way required and on any hardware platform. GINA's self-referential, multi-meta level foundation in combination with a new Vector Relational Data Model (VRDM) enables rapid development of information, analytical/computational modeling, system behavior, and decision support systems using model-driven architecture with executable component-based structures that eliminate the need for brittle code generation. The modeled SoS GINA solutions are comprised of a reconfigurable component topography with inherent data transparency.

Key GINA Concepts for SoS Modeling. A graphical representation of the GINA key concepts are illustrated in Figure 1.

Metarepresentation. A "supermetadata" model that completely describes system of systems (SoS) behavior is created using semantic information models.

Vector-Relational Data Modeling (VRDM). VRDM extends object-oriented software model to include relationships, necessary to create the metarepresentation.

VRDM-enabled Component Object Model. Special interfaces and components enable assembly of software structures that implement a metarepresentation as an executable model.

WorldSpace. The user is part of the model—Hypergraphs, maps of objects, and behaviors are created here and user requirements define the generative Network Architecture (gNA).

Metarepresentations. Metarepresentations—the abstracted descriptions of characteristics, services, and relationships ("supermetadata") of APIs, systems networks, etc.—completely describe the system of systems (SoS).

Multiple interoperating models, both metadata and software, enable metarepresentations to be assembled and executed for: control, development, application, component, and implementation.

Implementation. Software objects implement software models and use metadata models as assembly instructions for software components to create an executing implementation of the SoS model.

MMOWGLI

The Massively Multi-player Online War Game Leveraging the Internet (MMOWGLI) project develops and applies a browser-based application environment for conducting structured investigations of problems and issues of interest using crowd sourcing. MMOWGLI is an emerging methodology for rapidly obtaining ideas and problem solutions from large numbers of participants through web technologies. MMOWGLI provides "a text-based social networking platform that allows many users to interact directly with one another using web browsers in real time" (Guertin et al., 2013). MMOWGLI is "an online game platform designed to elicit collective intelligence from an engaged pool of world-wide players" (Zhao et al., 2013, p 498). The gaming environment has been used for online multi-player explorations into such diverse topics as Naval energy use and counter-piracy, in addition to its use for the Business Innovation Initiative used as the case study for this paper. During game execution, large quantities of data are collected regarding player actions and inter-relationships across players.

Data also provide information on the network connections used, allowing analysis of issues regarding who is connecting and from where.

The MMOWGLI game that was used for this effort was the Business Innovation Initiative (bii) game1. This game was designed and conducted to enable Navy and industry professionals to explore incentives and motivations on how best to improve the Navy's new Open Systems Architecture (OSA)2. Online players worked together to propose and publish new Idea Card Chains and Action Plans on how industry and the Navy can work together more effectively by motivating the Acquisition Work Force to employ OSA principles in its acquisition strategies.

Access and participation in the game were restricted to U.S. citizens. Users declare their affiliations and citizenship when registering for the game. All registrations are reviewed by game administrators and either permitted or disallowed. The sensitive nature of the global use of a DoD network game make the MMOWGLI game an excellent candidate for a GIS visual analytic application for rapid analysis and administrator situational awareness.

ATRAP

ATRAP is a powerful visual analytical tool developed by the Intelligence Battle Lab at Ft. Huachuca. ATRAP provides a visualization environment for viewing data relationships semantically, temporally, and geospatially. The analysis functionality that ATRAP provides includes: link analysis, ECA (enemy course of action) and DECA (derivative enemy course of action) templates which can be created and overlaid on the system dynamically, and the integration of heterogeneous data such as images, movies, audio files, and typed or tag-based selectable data. In a prior GINA model, the ATRAP system was near real-time enabled to collect data from smart phones to enhance situational awareness (Dolk et al. 2012). For this GINA application, ATRAP provides an environment for graphically displaying the geographic locations of users who participated in the MMOWGLI bii game.

APPROACH

Our approach for creating the cyber visual analytic application for near real-time network game participant GIS-monitoring is as follows:

1. Database preparation: Store MMOWGLI game data into a Structured Query Language (SQL) server for external access.

2. Obtain and integrate (into the MMOWGLI game database) geolocation data on Internet Protocol (IP) addresses occurring in the MMOWGLI data.

3. Parse username and IP address information from access log entries stored in the MMOWGLI game database.

4. Provide data access authority and password to servers on the NPS network to enable the GINA application server to access the MMOWGLI game database.

5. Design and develop GINA entities (Connections, XTypes, Elements, Vectors, Forms, etc.) to create a GINA-MMOWGLI application that is able to access and manipulate data from the MMOWGLI game database.

6. Configure the GINA-MMOWGLI application for data ingest by the ATRAP application.

MMOWGLI Game Database Preparation

MMOWGLI Game Database Design and Data Collection. All user actions during conduct of the MMOWGLI game are recorded in MySQL database tables for maintaining the game content for later analysis. For purposes of this project, the Business Innovation Initiative (bii) game database was copied to allow its manipulation separate from the official game database. The MMOWGLI bii database server can be accessed using username and password. MySQL and standard Structured Query Language (SQL) commands (e.g., show tables, create table, drop table, insert into, select, etc.) can be executed to examine and manipulate the database structure and content.

MMOWGLI Game Data Preparation. Using MySQL, a new table, AccessLogEntry, is added to the MMOWGLI MySQL bii game database to store the IP addresses and geographic location data. The geographic locations of IP addresses are added to the table by reading data provided by MaxMind (http://dev.maxmind.com/geoip/geolite). This operation results in population of clientLatitude and clientLongitude columns in the AccessLogEntry table.

Usernames and associated IP addresses are parsed from the game log entries for login events (eventtype = "1") stored in the GameEvent table. These entries have the general form *username on host from location / xxx.xxx.xxx.xxx,* where "host" is the name of the host computer used for the login, "location" is a verbal description of the location of the login (e.g., "Monterey California USA"), and "xxx.xxx.xxx.xxx" is the IP address associated with the login event (e.g., 172.20.81.41).

A GameLoginEvent table is created to store usernames, IP addresses, and timestamps from the login event records, as follows:

```
CREATE TABLE GameLoginEvent (ID
bigint(20), DateTime datetime, userName
varchar(255), IP varchar(15))
```

The usernames and associated IP addresses are parsed from these entries using the following SQL command:

```
INSERT INTO GameLoginEvent (ID,
DateTime, userName, IP)

SELECT ID, dateTime,

trim(substring_index(description,'
on', 1)), trim(reverse(substring_
index(reverse(description),'/', 1)))

FROM GameEvent where eventtype=1;
```

This command selects specific data from the GameEvent table to populate the columns of the GameLoginEvent table. While a join of the tables inside the MySQL database is straightforward using SQL commands, the tables (AccessLogEntry and GameLoginEvent) are kept separate in the source database to demonstrate the use of vectors in the GINA application.

Connecting Data Servers. Access to source databases is designated in GINA as Connections, with associated Sources and Columns corresponding to tables and columns from the source database structures. Each Connection provides access authority information (username and password) to enable the GINA application to log onto the source server. In the case of the bii data, there are multiple layers of access to be granted; first to the MMOWGLI MySQL server and then to the MySQL database itself. Since GINA is principally configured to work with a Microsoft SQL (MSSQL) database, system administrators implemented mechanisms to copy the MySQL data structures and contents into a MSSQL database for the GINA application to directly access. This setup is shown in Figure 2.

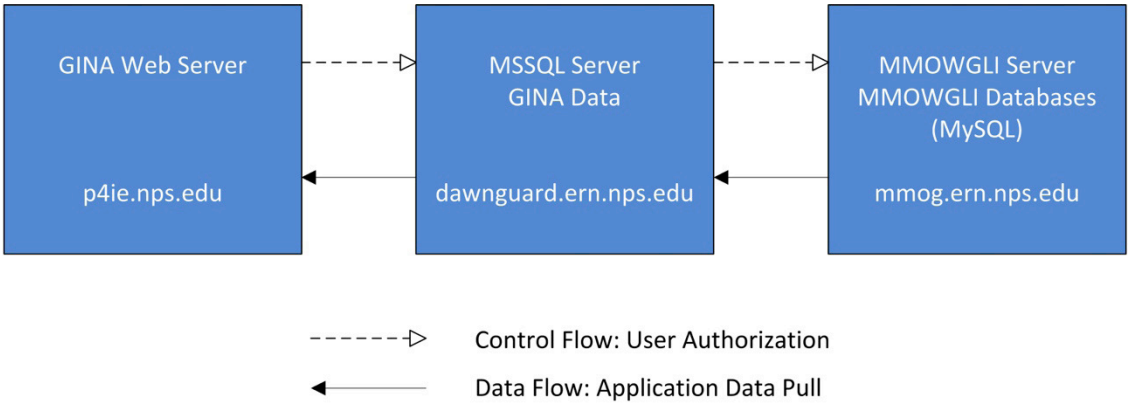

FIGURE 2. MMOWGLI GAME DATA IS REPLICATED FROM THE SOURCE SERVER TO PROVIDE A COPY DIRECTLY ACCESSIBLE BY THE GINA APPLICATION SERVER (GINA WEB SERVER).

GINA Application Design

The GINA application is constructed from the configuration of GINA Connections, Sources, Columns, XTypes, Elements, Vectors, Forms, Windows, Fields, and Modules that are specified in the web form user interface. An example of the GINA web form user interface for configuration of a GINA Connection for the MMOWGLI MySQL database server is illustrated in Figure 3. The specified attributes are stored in MSSQL and subsequently referenced and utilized as needed.

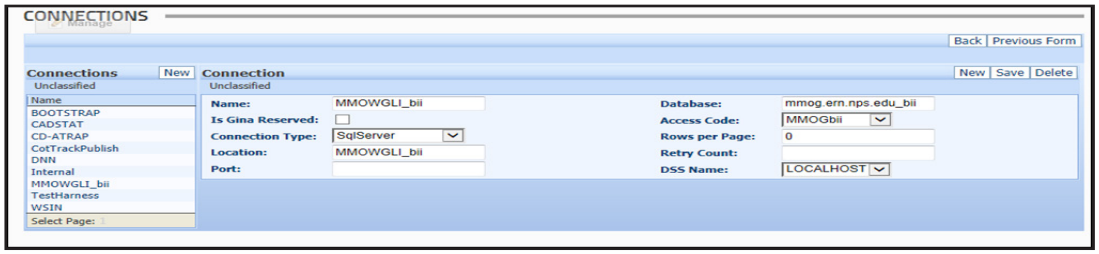

FIGURE 3. GINA WEB FORM USER INTERFACE FOR DEFINING THE MMOWGLI_bii CONNECTION.

The two tables in the MMOWGLI MySQL database server for this application are AccessLogEntry and GameLoginEvent. The first contains the IP address and location (latitude and longitude) of the IP address. The second contains the username and IP address of login events. Each of these tables and relevant table columns are specified in the GINA Sources portion of the UI and respective GINA Columns section. The list of Columns associated with each Source includes an id field from each of the source tables, providing for high-resolution transparency of the data model.

ATRAP Integration

Data Server Access. To enable the ATRAP application running on a laptop outside the NPS network to access the GINA database server inside the NPS domain, the authorized user establishes a VPN connection to NPS, starts the ATRAP application, and enters requisite credentials for the database.

GINA Application Preparation. For integration with ATRAP, two GINA model objects (XTypes) must be present in the GINA application: 1) an XType representing data from the GINA application (i.e., MMOWGLI bii game data of interest) and 2) an XType representing the ATRAP entity that will be populated from the GINA application. The GINA UI configured for the XType named mmbii_UserLocation is shown in Figure 4. This XType provides access to the username, IP address, and geographic location (latitude and longitude) of the IP address. Its associated self-reference Vector, also named mmbii_UserLocation, is defined in Figure 5.

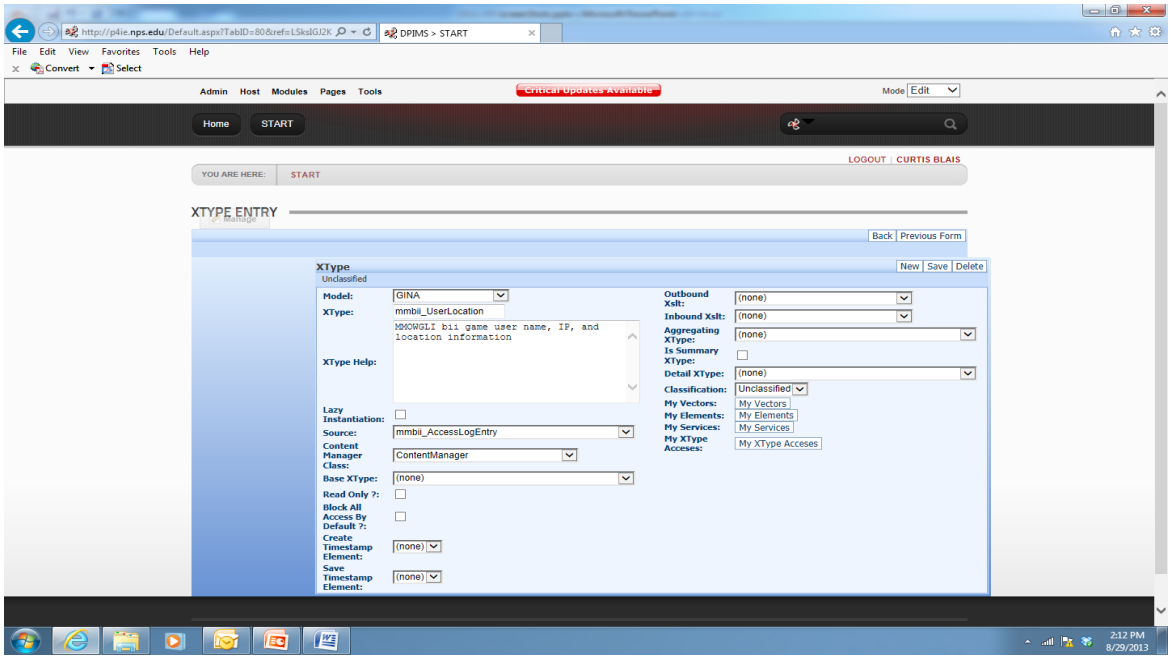

FIGURE 4. DEFINITION OF THE mmbii_USERLOCATION XTYPE FOR MMOWGLI bii DATA, INCLUDING USERNAME, IP ADDRESS, AND GEOGRAPHIC LOCATION.

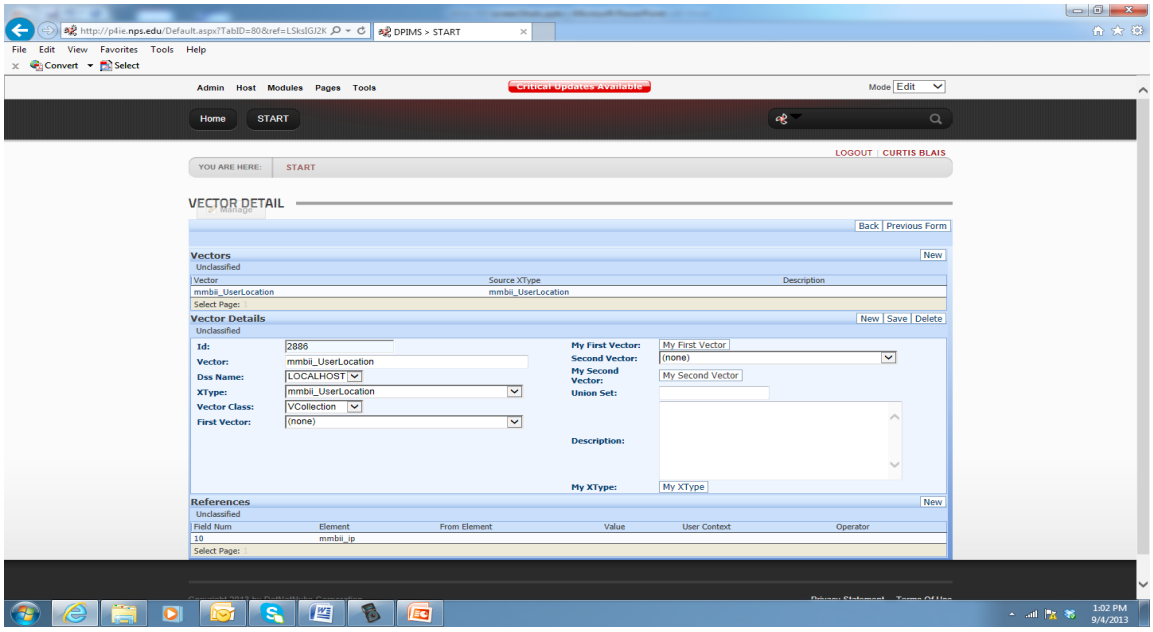

FIGURE 5. ASSOCIATED SELF-REFERENCE VECTOR FOR XTYPE mmbii_USERLOCATION.

The second XType, here named mmbii_ATRAP (Figure 6), provides representation of the ATRAP entity that will receive data from the GINA-MMOWGLI application. The Source of this XType is set to an existing Source in the GINA server; namely, IEDIncident, whose declaration is shown in Figure 7. The Content Manager Class is set to AtrapContentManager, a pre-existing class designed for the purpose of transferring data between GINA applications and the ATRAP application.

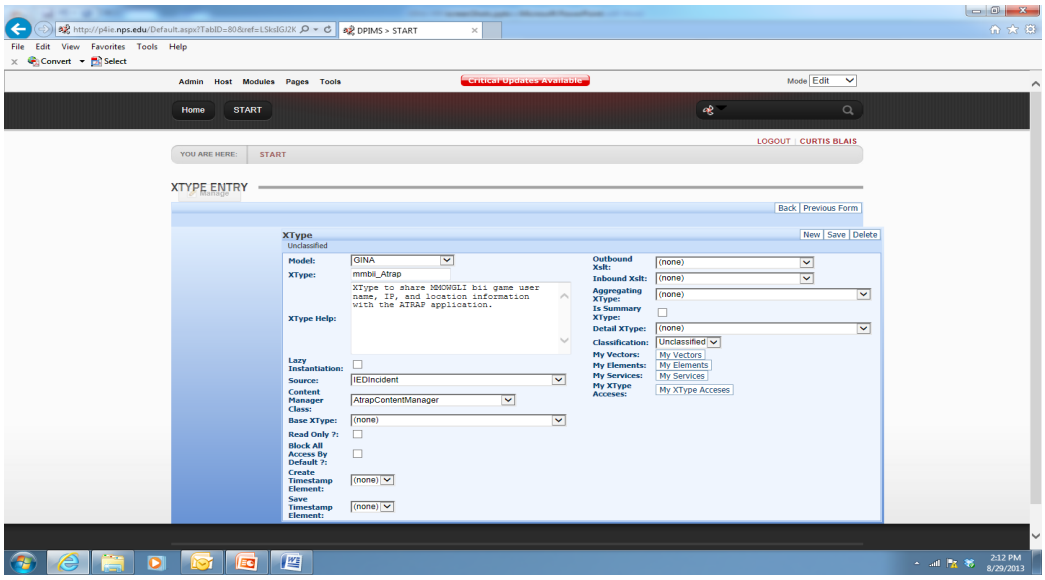

FIGURE 6. CONFIGURING AN XTYPE ASSOCIATING ATRAP ENTITY TO MMOWGLI bii GAME DATA.

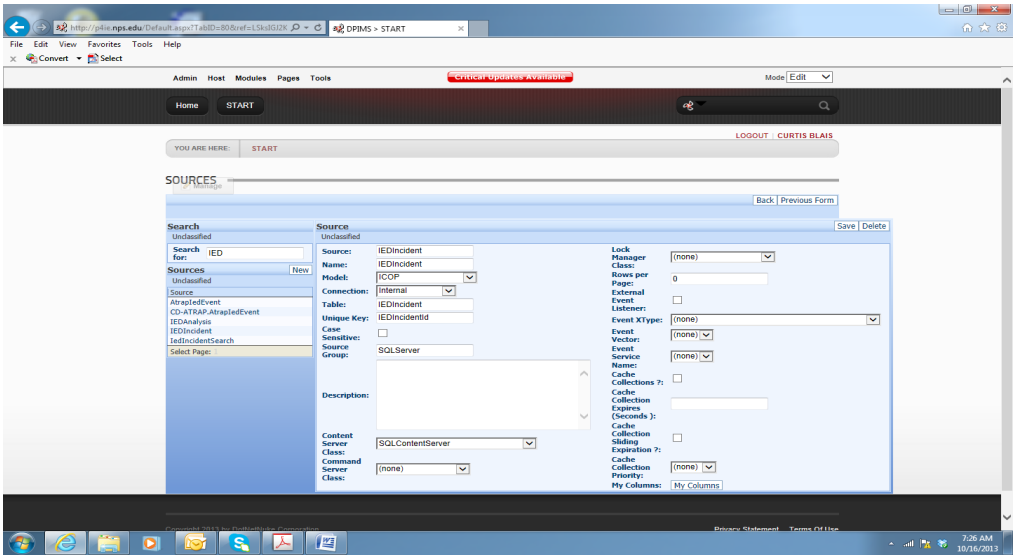

FIGURE 7. DECLARATION OF THE IEDINCIDENT SOURCE USED FOR POPULATING GINA CONTENT FROM THE ATRAP APPLICATION.

The mmbii_ATRAP XType requires a specific set of Elements to correspond to fields in the ATRAP entity representation. These Elements are defined for the mmbii_ATRAP XType in Table 1.

ATRAP Entities. The GINA model is configured to access ATRAP and to allow access to the user and user location data. To perform this, the following steps are executed:

In ATRAP, we define a new Entity Type (Event, Equipment, Location, Organization, Person, or Undefined) by selecting Tools / Data Editors / Entity Type Editor in the menu bar. We select Undefined, and enter the name and description of entity type mmbiiUser, then save to the ATRAP_SOARING_ANGEL database. In the ATRAP tools menu, we then define attributes of the new entity type username, IP, latitude, and longitude.

From the ATRAP database, the global unique identifier (guid) of the new Type for the mmbii_Atrap XType's EntityTypeId element is used to set the default value of the EntityTypeId element (Figure 8). SQL commands are used to update and enable the selection of entity attributes within ATRAP.

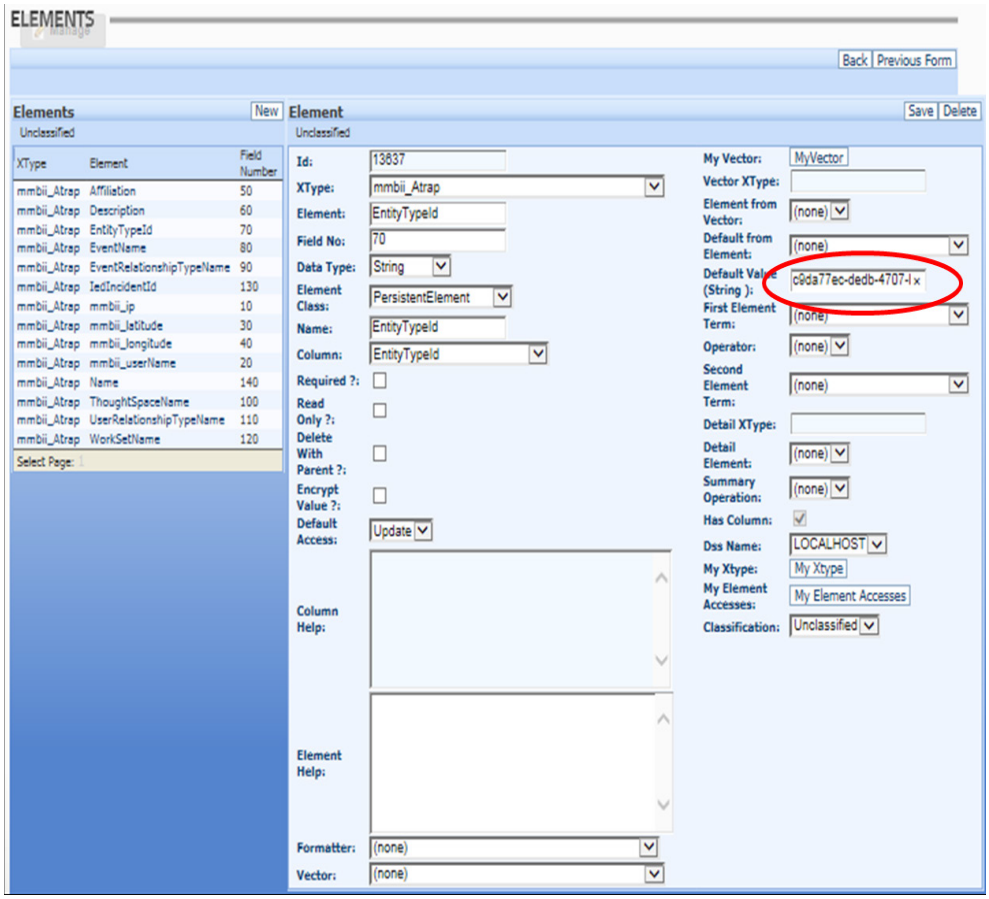

FIGURE 8. SETTING THE DEFAULT VALUE FOR THE ENTITYTYPEID ELEMENT OF THE mmbii_ATRAP XTYPE.

Service Chaining from the mmbii_UserLocation XType to the mmbii_Atrap XType. A chain of services is defined in GINA to move data from the MMOWGLI application to the ATRAP application. This begins with configuration of a form in the GINA UI, named here mmbii_UserIPLocation, for the mmbii_UserLocation data. We create the "Save to ATRAP" button on the form by specifying Service(s) in each XType and a Command Collection in the mmbii_UserLocation XType. Figure 9 shows configuration of a service for the mmbii_UserLocation XType, followed by configuration of services on the ATRAP mmbii_Atrap XType in Figures 10 and 11.

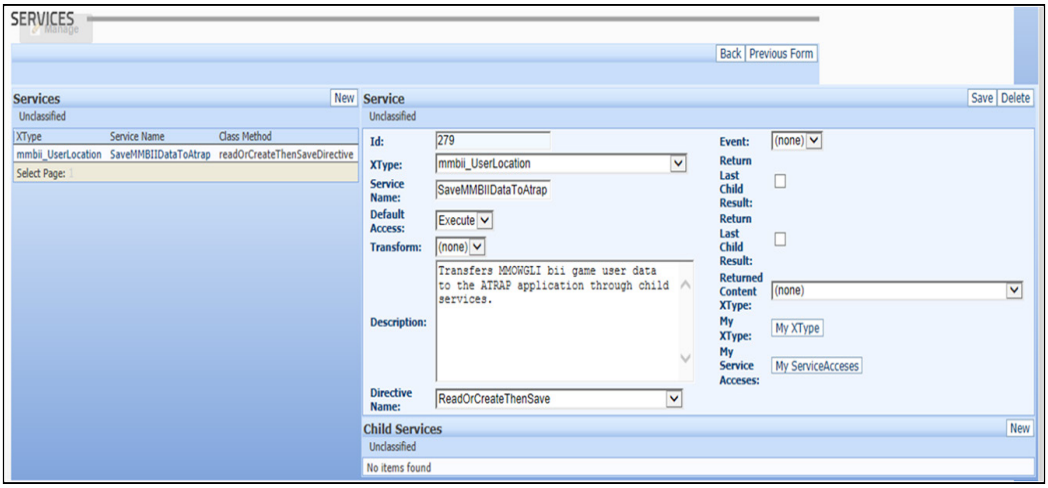

FIGURE 9. CONFIGURATION OF THE SAVEmmbiiDATATOATRAP PARENT SERVICE ASSOCIATED WITH XTYPE mmbii_USERLOCATION.

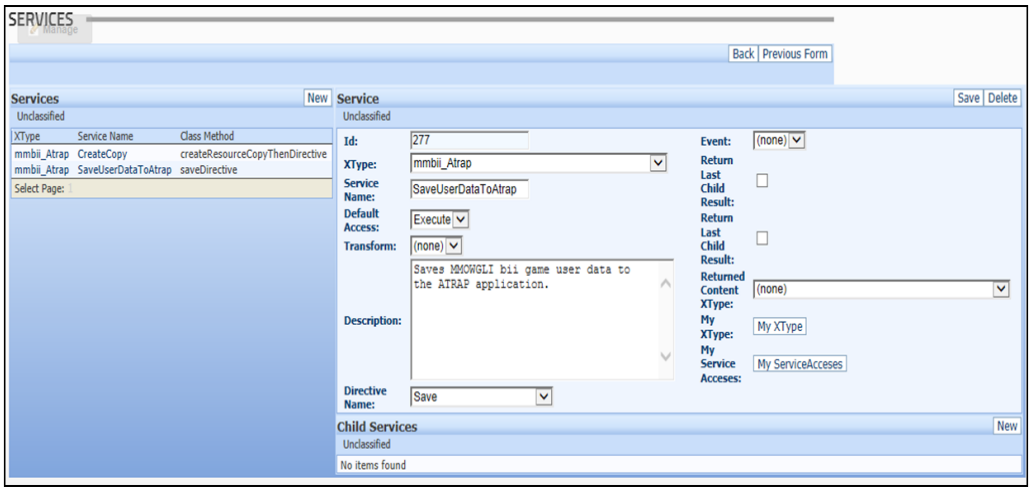

FIGURE 10. CONFIGURATION OF THE CREATECOPY INTERMEDIATE SERVICE ASSOCIATED WITH XTYPE mmbii_ATRAP.

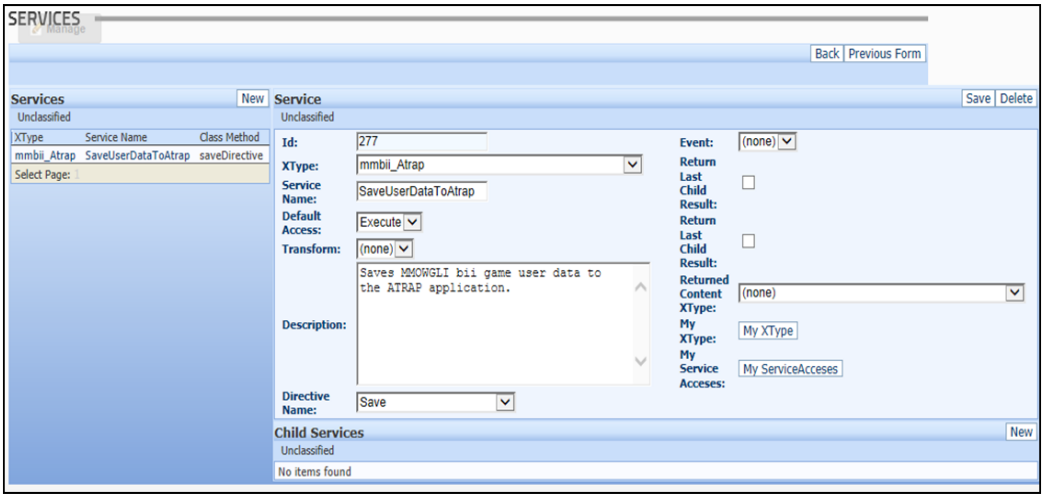

FIGURE 11. CONFIGURATION OF THE SAVEUSERDATATOATRAP CHILD SERVICE ASSOCIATED WITH XTYPE mmbii_ATRAP.

The chaining of services is accomplished through service maps, accessed by selecting "New" in the Child Services area of the GINA form. The chaining of services SaveMMBIIDataToAtrap (top-level) to CreateCopy (intermediate service, child to SaveMMBIIDataToAtrap) and CreateCopy to SaveUserDataToAtrap (child service to CreateCopy) are accomplished using the GINA Service Maps form.

Creating the Command Collection. In order to create the executable behavior for a GINA UI e.g. 'go button,' the behavior is specified as a Command Collection. In the GINA UI, the command properties are configured in the Commands form. Here a Command Button can be added to the form with a selected Command Collection. This is an example of using GINA UI to create further GINA functionality through configuration, without recompiling the system or restarting the system.

GINA-MMOWGLI APPLICATION OPERATION

Starting the Application

The GINA-MMOWGLI application is accessed via a web browser (Internet Explorer, Mozilla, etc.). Following the login, the screen displays the GINA UI Application window. Clicking on the "Start" button will navigate to the GINA UI "SELECT APPLICATION" form. Click on "Training" and the GINA UI "SELECT MODULE AND FORM" form is displayed. The MMOWGLI module may be selected here from the Application Modules list. The Module Details portion of the form identifies the forms that are assigned to the MMOWGLI module: mmbii_AccessLogEntry; mmbii_UserIPLocation; mmbii_UserLocation; mmbiiGameEvent; and "User Name to Location."

From the GINA MMOWGLI module, the various forms may be selected. The mmbii_AccessLogEntry form provides a listing of IP addresses and their associated geographic location. The geolocation of the first IP address in the list appears in the detail window at the bottom of the screen. Clicking on any of the IP addresses in the list will bring up the corresponding location in the form. The mmbiiGameEvent form provides a list of usernames and associated IP addresses. Clicking on a username in the upper window of the form brings up the associated IP address in the lower window of the form. Selecting the IP address then brings up associated geo-location on the form. The mmbii_UserLocation form provides a list of IP addresses with associated usernames and geographic locations. As above, clicking on an IP address in the upper window of the form brings up the associated username and geographic location in the lower window of the form.

An additional form was specified to demonstrate a search capability that would draw information from across the different systems and present it as if from a unified system. To obtain data in the form, a search string is entered (all or part of a username) in the "Search for" block on the form (Figure 12). This will yield all users with string matches, and then populate associated geo-location and IP address.

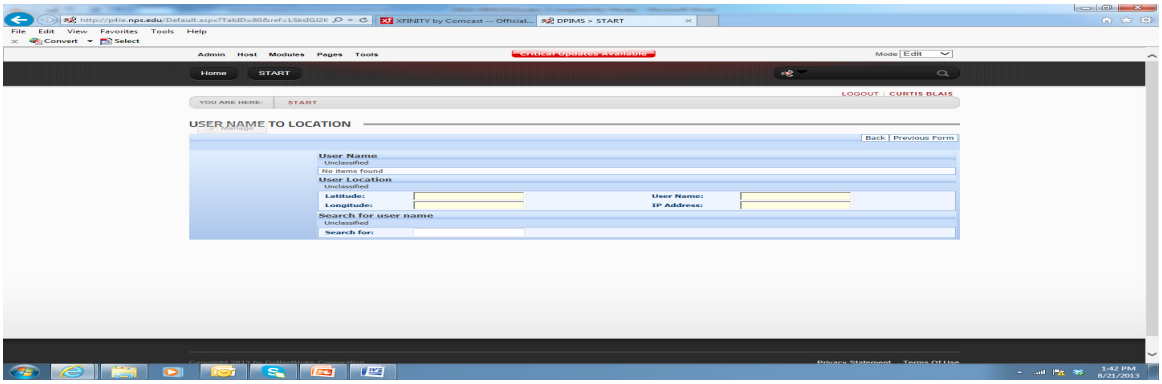

FIGURE 12. SCREEN SHOT OF THE "USER NAME TO LOCATION" SEARCH FORM FROM THE MMOWGLI MODULE.

Near Real Time Data Visualization

The ATRAP program is a sophisticated event analysis program with several visual analytic capabilities including link analysis and 3d GIS (Figure 13). There was no further development of the ATRAP expert system for this use case where it is utilized as the visualization and analysis component of the GINA-MMOWGLI application. The MMOWGLI user location data may now be fully utilized in near real-time by ATRAP for event, link, GIS analysis and benefit from the power of understanding the information in a space and time context with known threats.

Any change or modification to this SoS model, e.g., utilizing a different visualization, may be implemented through specification of the GINA model without compiling, redistribution of executable, or rebooting. This capability to configure SoS allows government and industry flexibility when facing redundant expert system capability across the distributed mission space. This allows for legacy and new systems to be utilized without regard for standardization, and also allows for organizational or departmental, right down to individual analyst's choice of system components. The high-resolution data access, down to a particular column of a particular database, allows for precision control of information when it comes to multi-level or compartmentalized information as well.

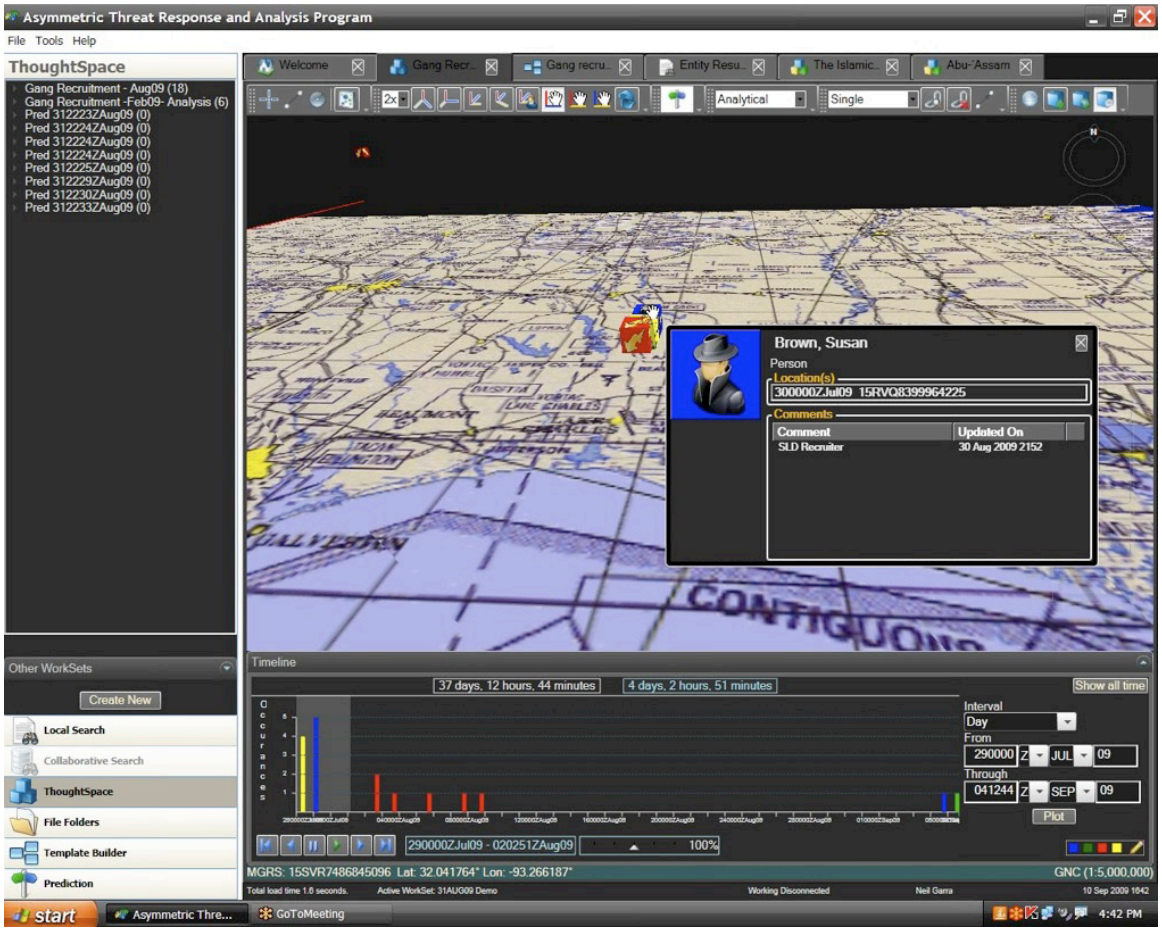

FIGURE 13. ATRAP DATA VISUALIZATION SHOWING EVENT CUBES IN TIME (Z-AXIS) MAPPED TO GEOLOCATION (X-Y AXIS). THIS IS JUST ONE VIEW AND ASSOCIATED EVENT TIME LINE THAT IS AVAILABLE IN ATRAP.

CONCLUSION

This project demonstrated the use of GINA to create a System of Systems in the cyber domain specifically to read and process data from the MMOWGLI bii game into a GIS analysis tool in near real-time. We configured an information model in the GINA web form UI that utilized the sub system components; in this case these were the expert systems: MMOWGLI and ATRAP. Further, the executable behavior of this application was configured within the GINA UI as well. The resulting capability of being able to monitor the users of the MMOWGLI internet game and derive geo-spatial associated information for realizing in both text based, and chosen GIS visualization (ATRAP). The system components (ATRAP and MMOWGLI) were not modified to work together; all manipulation and syntax matching was configured in GINA. The result is a configured extensible visualization capability for cyber domain that may be further modified for extended use or custom analysis tools through further configurations, not programming.

Additional analytics, such as alerting users for IP locations in certain countries, can be readily added to GINA through software services or as queries in the ATRAP application. This tool for development of applications dealing with manipulation and analysis of data from one or more sources offers extreme extensibility and customization that can evolve with changing technology and mission landscape.

TABLE 1.

mmbii_ATRAP XTYPE REQUIRED SET OF ELEMENTS THAT CORRESPOND TO FIELDS IN THE ATRAP ENTITY REPRESENTATION.

Element Number	Name	Data Type	Notes
Value 1	mmbii_userName	Persistent String	This column MUST be added to the IedIncident Table and Source in the ATRAP application
Value 2	mmbii_ip	Persistent String	This column MUST be added to the IedIncident Table and Source in the ATRAP application
Value 3	mmbii_latitude	Persistent String	This column MUST be added to the IedIncident Table and Source in the ATRAP application
Value 4	mmbii_longitude	Persistent String	This column MUST be added to the IedIncident Table and Source in the ATRAP application
Special 1	Affiliation	Persistent String	Default = U: set to "cdatrap"
Special 2	Description	Persistent String	Can be defaulted to any value or use a subformatter to get other element values
Special 3	EntityTypeId	Persistent String	This one must be defaulted to the GUID of the EntityType from the ATRAP application, as discussed later
Special 4	EventName	Persistent String	Can be defaulted to any value or use a subformatter to get other element values
Special 5	EventRelationshipTypeName	Persistent String	Default = Is Location For
Special 6	ThoughtSpaceName	Persistent String	Default = All Entities
Special 7	UserRelationshipTypeName	Persistent String	Default = Is Author Of – this defines the relationship of the user entering the data to the data
Special 8	WorkSetName	Persistent String	Default = Soaring Angel – you can make choices here
Special 9	IedIncidentId	Persistent GUID	Default = NewGuid
Special 10	Name	Persistent String	Default from an element that will show up as the header of your tile in ATRAP

REFERENCES CITED

Big Kahuna Technologies, LLC. (2009, October). Vector Relational Data Modeling (VRDM) User's Manual. Release 0.18.

Boulos, M., Viangteeravat, T., Anyanwu, M., Nagisetty, V., & Kuscu E. (2011). Web GIS in practice IX: A demonstration of geospatial visual analytics using Microsoft Live Labs Pivot technology and WHO mortality data. International Journal of Health Geographics, 10. 19

CNN Wire Staff. (2011, January 14). Homeland Security chief cancels costly virtual border fence. Retrieved from http://www.cnn.com/2011/US/01/14/border.virtual.fence

Cohort 19/Team Bravo. (2013, June). Viable short-term directed energy weapon naval solutions: A system analysis of current prototypes, NPS Systems Engineering Capstone Project Report. Naval Postgraduate School.

Dolk, D., Anderson, T., Busalacchi, F., & Tinsley, D. (2012). "GINA: System Interoperability for Enabling Smart Mobile System Services in Network Decision Support Systems." Proceedings of the 45th Hawaii International Conference on System Sciences. Maui, Hawaii.

Ephibian. (2011b). ATRAP Version Description Document v3.1. Ephibian, Inc. The Arizona Board of Regents on Behalf of the University of Arizona.

Guo D. (2007). Visual analytics of spatial interaction patterns for pandemic decision support. International Journal of Geographical Information Science, 21(8), 859–877.

Hicks, Richard. (2013, June 18). Monitoring and blocking network access based on geographic location using Forefront Threat Management Gateway (TMG) 2010. Retrieved from http://www.isaserver.org/articles-tutorials/configuration-security/monitoring-blocking-network-access-based-geographic-location-using-forefront-threat-management-gateway-tmg-2010.html

Hidalgo C. (2010). Graphical statistical methods for the representation of the human development index and its components. United Nations Development Programme, Human Development Reports Research Paper 2010/39.

Kanaracus, C. (2012). Air Force scraps massive ERP project after racking up $1B in costs. Retrieved from http://www.computerworld.com/s/article/9233651/Air_Force_scraps_massive_ERP_project_after_racking_up_1B_in_costs

Keim D., Robertson G., Thomas J., &van Wijk, J., (2006). Guest editorial: Special section on visual analytics. IEEE Transactions on Visualization and Computer Graphics, 12(6):1361–1362.

Scott, Amy. (2013, October 24). Obamacare: What we have here is a failure to integrate. Marketplace. http://www.marketplace.org/topics/health-care/obamacare-what-we-have-here-failure-integrate

ENDNOTES

1 The MMOWGLI bii game portal is found at http://portal.mmowgli.nps.edu/bii. A portion of the discussion in this section of the document is adapted from that web site.

2 An overview of the Open Systems Architecture is provided on the MMOWGLI site at https://portal.mmowgli.nps.edu/c/document_library/get_file?uuid=3b7db976-9a4e-4f54-8ebb-c8df5225dfeb&groupId=10156. Also see: http://www.acq.osd.mil/se/initiatives/init_osa.html.

ACKNOWLEDGMENT

This work was sponsored by USACE ERDC TEC and ASA (ALT). The GINA architecture is made available to DoD through a Cooperative Research and Development Agreement with Big Kahuna Technologies.

AUTHORS

Thomas Anderson (thomas.anderson5@us.army.mil) holds a PhD in seismology from the University of Connecticut. Anderson is a lead research scientist at the Engineer Research and Development Center (ERDC) Cold Regions Research and Engineering Laboratory (CRREL) and is liaison to the U.S. Army Training and Doctrine Command (TRADOC) Analysis Center, Monterey (TRAC - MTRY) at NPS (since 2007). Anderson also leads the Executable Modeling and Analysis project at TRAC – MTRY and developed the GINA Dragon Pulse Information Management System (DPIMS) specification and had it DIACAP-certified for strategic positioning as a baseline operational capability in DoD. His research interests include information modeling with GINA specifications applied to modeling system fusion, modeling visualization, and data modeling. Key aspects of this are knowledge management and multi-component decision analysis. Current use case domains are ISR, Operational Research and Cyber domains.

Curtis L. Blais (clblais@nps.edu) is a research associate and PhD student in the Naval Postgraduate School (NPS) Modeling, Virtual Environments, and Simulation (MOVES) Institute with over 30 years of experience in development of military war gaming and C4I simulation software, including over 20 years

of experience in management of a professional engineering staff. As a research associate for MOVES, he has managed and performed research on a number of projects related to advanced modeling and simulation (M&S) technologies. His teaching assignments include introduction and advanced courses in Extensible 3D Graphics (X3D) and the Extensible Markup Language (XML). His research interests include agent-based simulation and application of Web-based technologies to military M&S and C4I systems for knowledge representation and information exchange.

Don Brutzman (brutzman@nps.edu) is a computer scientist and associate professor working in the MOVES Institute at the Naval Postgraduate School in Monterey, California. Currently, he cochairs the Extensible 3D (X3D), X3D CAD and X3D Earth Working Groups for the Web3D Consortium. Together with Len Daly, he is coauthor of the book *X3D Graphics for Web Authors,* published April 2007 by Morgan Kaufmann. He is principal investigator for MMOWGLI sponsored by the Office of Naval Research (ONR). He is a retired naval submarine officer. His research interests include underwater robotics, real-time 3D computer graphics, artificial intelligence, and high-performance networking.

Scott A. McKenzie (samckenz@nps.edu) is a retired naval aviator with a master's degree in Systems Engineering Management from NPS. As an NPS faculty member for the Distributed Information Systems Experimentation (DISE) Research Group, he has led several successful applied research projects, including one that provided a "Blue Force" tracking capability on a common tactical picture for the Salinas Police Department. For the past year, McKenzie has been actively engaged with emergency response agencies, at all levels of government, gathering requirements for collaborative emergency response and applying GINA modeling toward building Systems of Systems that maximize the efficiency of information exchange efforts.

The New Demands of Online Reputation Management

Shannon M. Wilkinson | Editing and Research by Christopher Hampton

ABSTRACT

The explosive growth of the Internet has dramatically changed the demands of reputation management. There are few barriers to publishing online, and every author has at least the potential of reaching broad audiences. There are also few laws regulating online information. Content is often posted anonymously, and website operators have legal immunity over what is posted on their sites. In many cases there is no one to prosecute, and no leverage to demand retractions.

Online reputation management (ORM) first appeared in the mid-1990s, and has grown along with Internet use. These changes have also forced a much more proactive stance toward the protection of brand integrity. Security professionals now have a broad mandate for investigating, addressing and resolving online threats to the reputation of their company and its executives.

This paper gives an overview of the leading online reputational threats faced by companies in the United States, as well as an explanation how such events unfold, the motivations behind them, and how they can be protected against and resolved. Threats discussed range from the dissemination of the home addresses and family information of executives to the leaking of internal company documents by inside sources, targeted online defamation campaigns, and the impersonation of executives on social media and other platforms, in addition to more conventional public relations crises.

The best tactics for avoiding many of those crises are of the proactive variety. They include online monitoring of the company brand and executives' online presence, as well as of social media sites maintained by family members. Company executives, in particular, should be made aware of online security practices, including protecting their data and using encryption for online correspondence. Most importantly, the company should establish a strong online presence, including interactive forums where company representatives can address grievances.

Effective planning will protect a company against many reputational threats. Reactive ORM techniques are increasingly focused on the production of quality content. The manipulation of search engine results—what used to be considered the central activity of ORM firms—has lost its utility as search engine algorithms have grown more sophisticated.

THE NEW DEMANDS OF ONLINE REPUTATION MANAGEMENT

The EU's recent passage of the "Right to Be Forgotten" law gives European citizens the ability to force Google and other search engines to remove links to embarrassing or irrelevant information.

The passage of that law increases the contrast between legislation regarding online publishing in Europe and the United States. In the U.S. there are still very few legal boundaries constraining the publication and distribution of online content. Authors are free to post almost any material anonymously.

If anyone finds material to be damaging, they have little leverage to demand a retraction and no clear target for prosecution. Discussion about new legislation has revolved around freedom of speech issues, issues that have advocates including such well-funded organizations as the Electronic Frontier Foundation.

In the U.S., the main law governing the Internet is Section 230 of The Communications Decency Act, which frees website owners from legal responsibility for what others post on their sites. It states, "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider."

Understanding the implications of that law and how it impacts the privacy, security, and reputations of U.S. citizens is recommended for cyber professionals. Security professionals now have a broad mandate for investigating and addressing online threats to the reputation of their company and its executives. Their employers and colleagues often seek their guidance in mitigating the many issues that result from the types of defamation, embarrassment, and physical security risks that have become a common occurrence online. Today all major corporations and public companies have cyber departments within their security and investigations departments. The FBI has a cyber investigations unit, as do the law enforcement departments of most major cities.

SHORTCOMINGS OF CURRENT LEGISLATION

Passed in 1996, Section 230 has not been updated to accommodate the new platforms and new types of social behavior found online. It does not adequately protect individuals from defamation, from the widespread publication of their age and home addresses, or from the harm that can result from both.

In the absence of legal protections, there are a range of strategies that individuals and companies in the U.S. can put in place to safeguard their reputations online. This paper gives an overview of the leading online reputational threats, as well as an explanation of how such events unfold, the motivations behind them, and ways they can be protected against and resolved.

Before explaining these strategies, it is important to clarify what online reputation management is, how it differs from reputation management (which addresses corporate culture rather than Internet content), and how the aggregation and social sharing of information on the Internet contributes to ORM issues.

THE ONLINE REPUTATION MANAGEMENT INDUSTRY

The online reputation management industry first appeared in the mid-1990s. From that point, it has grown in step with the Internet. ORM is popularly known as a service that repairs reputational damage caused by malicious anonymous commentary posted on Internet sites. Some ORM firms claim to improve reviews of businesses online (on sites such as Yelp). Others promise to push unwanted Internet content onto lower pages of search results. But the field is much broader, and the best firms use a range of techniques to protect and build a client's brand. A range of such companies can be viewed by Googling "online reputation management" and scanning the first five pages of results.

Like the Internet as a whole, the online reputation management business is largely unregulated. As a result, instances of extortion by disreputable ORM providers have been well-documented in the media (Krause, 2014). For instance, any individual who has been arrested may be approached by an ORM provider offering to control the dissemination of a mug shot. If the provider isn't contracted, it may disseminate that mug shot itself (Connelly, 2012).

Some ORM providers offer marketing services. They use a combination of content, technology, and SEO (search engine optimization) to influence where a company's marketing materials appear in search results. The effectiveness of this approach can be impeded by the continually evolving algorithms Google and other search engines use to determine

how results are ordered. (Visit Google's "How Search Works" for more information, http://www.google.com/insidesearch/howsearchworks/thestory/)

REPUTATION MANAGEMENT

Online reputation management is often confused with "reputation management," which refers to the broader task of maintaining the public integrity of an organization's or individual's brand. Reputation management has exploded as an industry during the last ten years because of the rise of social media and the transparency it engenders, as well as the increased ability of citizens and consumers to comment publicly on behavior, policies, and products. In addition to encompassing communications and public relations (including crisis management), reputation management is also a lucrative consulting practice that spans the review of every aspect of a company's internal structure to ensure its culture and practices adhere to and reflect a company's values (which includes best-practice management and procedures).

COMMON ONLINE REPUTATION THREATS FACING U.S. COMPANIES

Examples of online reputation threats that are commonly experienced by companies and organizations in the U.S. include:

- Public databases publishing executives' home addresses and information on family members. Once this information appears on one database, it is often harvested and disseminated through other outlets. This is not just a privacy issue; it can pose security risks as well.
- Publication of privileged emails and internal company documents that were leaked by inside sources.
- Organized online defamation campaigns.
- Being the subject of domain squatting: Registering or using a domain name ("[your name].com"), then offering to sell the domain to the person or company who owns the trademark at an inflated price, or using the domain. Donald Trump was the subject of such an attack, and successfully sued for removal of the websites (Draznin, Haley, 2014).
- The impersonation of executives on social media and other online platforms. This can be a particularly damaging offshoot of domain squatting. It can be prevented by reserving appropriate handles in major social media platforms.
- Targeting of family members who have shared (perhaps too much) personal information on social media outlets.
- Being the subject of parody websites that criticize and lampoon CEOs and other public figures.

As a specialist working in this field, I have encountered each of these threats. I have seen: emails from top executives at public companies get extracted from the company's secure digital archives and published in online forums; organized Twitter campaigns sending out multiple Tweets daily with links to defamatory false content about public figures; satellite photographs of the homes of high-profile executives published online with maps and directions to their homes and messages for readers to do them harm; and nude images of executives posted on multiple websites and social media platforms prior to a quarterly earnings release. Such cases are not usually publicized.

Common sources of threats include retaliation from severed business, social, or personal relationships (most often dissatisfied or dismissed employees). Threats also include competitors, industry bloggers who will benefit from the attention they receive, unhappy customers whose attempts to assuage their complaints through company channels have failed, individuals or groups with different political or social views, or simply anonymous "trolls" (people

who cultivate discord on the Internet by posting inflammatory, extraneous, or off-topic messages in an online community).

Some threats can propagate online for months before being noticed. Most start on lower pages of Google and can take weeks to rise to a prominent position on page one of a Google search. Often company leadership becomes aware of them only when a crisis point is reached and it threatens to disrupt a brand or an individual's credibility.

Cyber security experts are often turned to in such situations. The communications departments of some companies, or executives charged with managing a firm's reputation (a growing practice), are also resources used to mitigate such issues. In some cases CEOs or another C-Suite executive ask their security directors to conduct an investigation to unearth the identity of the perpetrator. Forensic cyber investigators—which growing numbers of law firms and investigative companies employ—can often identify the individual responsible for posting defamatory and other inappropriate content online. In some cases, they partner with cyber specialists in law enforcement, particularly when they have relationships with that sector due to prior employment with Federal agencies such as the Secret Service or F.B.I. However, not all such posters can be easily identified.

It can be difficult to locate legal information sufficiently informative to indicate whether an online reputation issue meets the legal requirements of "defamatory" that are necessary to take legal action. Not all companies (or individuals) want to take such public action, either. An example of one successful lawsuit occurred in 2013, when a Harvard graduate was charged with online fraud, impersonation, and harassment (Leland, John, 2013).

One useful reference source for Internet legal information is the Chilling Effects Clearinghouse, a joint project of the Electronic Frontier Foundation and Harvard, Stanford, Berkeley, University of San Francisco, University of Maine, George Washington School of Law, and Santa Clara University School of Law clinics. This excerpt from their website explains their point of view:

> Chilling Effects aims to help you understand the protections that the First Amendment and intellectual property laws give to your online activities. We are excited about the new opportunities the Internet offers individuals to express their views, parody politicians, celebrate their favorite movie stars, or criticize businesses. But we've noticed that not everyone feels the same way. Anecdotal evidence suggests that some individuals and corporations are using intellectual property and other laws to silence other online users. Chilling Effects encourages respect for intellectual property law, while frowning on its misuse to "chill" legitimate activity. (www.chillingeffects.com)

The extensive Boolean-format database of the Chilling Effects Clearinghouse provides quick searches of an exhaustive range of topics. The Electronic Frontier Foundation's website also has substantial information about Internet legal rights (www.eff.org). The following is an excerpt from its Bloggers' FAQ on Online Defamation Law, found in its Legal Guide for Bloggers' section:

> What is defamation?
>
> Generally, defamation is a false and unprivileged statement of fact that is harmful to someone's reputation, and published "with fault," meaning as a result of negligence or malice. State laws often define defamation in specific ways. Libel is a written defamation; slander is a spoken defamation.
>
> What are the elements of a defamation claim?
>
> The elements that must be proved to establish defamation are:
>
> 1. a publication to one other than the person defamed;
>
> 2. a false statement of fact;

3. that is understood as

a. being of and concerning the plaintiff; and

b. tending to harm the reputation of plaintiff.

If the plaintiff is a public figure, he or she must also prove actual malice. (www.eff.org)

Google Executive Chairman Eric Schmidt and Google Ideas Director Jared Cohen address issues of defamation and privacy in *The New Digital Age: Reshaping the Future of People, Nations and Business* (Schmidt & Cohen, 2013):

> Smear campaigns and online feuds typically involve public figures, not ordinary citizens… our ability to influence and control how we are perceived by others will decrease dramatically.… The shift from having one's identity shaped off-line and projected online to an identity that is fashioned online and experienced off-line will have implications for citizens, states and companies as they navigate the new digital world.… Identity will be the most valuable commodity for citizens in the future, and it will exist primarily online. (pp. 32-36)

DATA SCRAPING RESULTS IN SERIOUS PRIVACY INVASIONS

Data scraping – the automated collection, indexing, and publishing of online data– results in vast amounts of personal information about millions of individuals being available in "people" databases like Intelius and Spokeo, which package and sell it for nominal amounts ($10 or less). Many people, including high-profile targets, do not even realize their home addresses, ages, and family members' names are widely available on such sites. But it can lead to serious physical security risks.

CONCLUSION

The best tactics for avoiding many of those crises are proactive ones. They include online monitoring of the company's and executives' online presence, as well as social media sites maintained by executives' family members. Numerous social media monitoring companies now provide such services, and Google alerts can be set up (for free) to monitor any keyword. (Due to a potentially high volume of daily alerts that may come into email boxes, setting up a designated email address just to receive alerts is recommended.) Company executives in particular should be made aware of online security practices, including protecting their data, using encryption for online correspondence, and ensuring they avoid letting emails sit in their Gmail and other personal email boxes. Such emails are not only hacking targets, but can lead to the type of career-ending crisis as happened to General Petraeus. VIPs, including industry leaders, should place their real estate holdings in private trusts and buy any new properties through those trusts, which will help keep their private addresses from publicly available databases.

The most important tool for protecting against reputational crises is establishing a strong online presence. For companies, this should include forums where company representatives interact directly with customers to address grievances. Statistics show that the more options consumers have to air grievances in online settings provided by organizations, the less likely they are to vent in public forums, which can produce viral (and possibly justified) rants.

Effective planning can protect a company against many reputational threats. Reactive ORM techniques are increasingly focused on the production of quality content. The manipulation of search engine results—what used to be considered the central activity of ORM firms—cannot be guaranteed as search engine algorithms have grown more sophisticated and are continually being updated.

The best policies integrate strong security measures with a strategic and ongoing engagement with the Internet. Building a strong and authentic online presence not only allows a company to avert or respond to reputational crises; it is also a very effective way to build a brand and relationships with customers.

REFERENCES CITED

Connelly, C. (2012, December 23). Mug shot websites charge when you're charged, for now. NPR. Retrieved from http://www.npr.org/blogs/thetwo-way/2012/12/23/167916738/mug-shot-websites-charge-when-youre-charged-for-now

Draznin, H. (2014, March 2). Trump awarded damages in 'cybersquatting' case over domain names. CNN. Retrieved from http://www.cnn.com/2014/03/01/studentnews/trump-cybersquatting-lawsuit/

Krause, K. (2014, March 27). Former Texas resident charged with extortion for threatening to destroy client's online reputation. *The Dallas Morning News*. Retrieved from http://crimeblog.dallasnews.com/2014/03/texas-man-charged-with-extortion-for-threatening-to-destroy-a-former-clients-online-reputation.html/

Leland, J. (2013, February 16). Online battle over sacred scrolls, real-world consequences. *The New York Times*. Retrieved from http://www.nytimes.com/2013/02/17/nyregion/online-battle-over-ancient-scrolls-spawns-real-world-consequences.html?ref=nyregion&_r=1&#comments

Schmidt, E. & Cohen, J. (2013). *The new digital age: Reshaping the future of people, nations and business*. New York: Knopf.

AUTHOR

Shannon Wilkinson (sw@reputation-communications.com) is founder and CEO of Reputation Communications, an online reputation management firm providing services to CEOs, industry leaders, V.I.P.s and their organizations. Wilkinson blogs at *You Online*. She is the author of *Online Reputation Management: What Every Influencer Needs to Know*, an annually updated guide for newsmakers. A *Forbes* contributor, Wilkinson is a public speaker and a media resource for information regarding online reputation management practices. She tweets at @reputationnews and @shannonnewyork.

Christopher Hampton is a publishing professional based in New York City.

The Risk of Cyber Crimes to the Critical National Infrastructure: A Threat Assessment

Brian A. Lozada

ABSTRACT

Cyber crimes and cyber espionage are increasing risks to the United States' economic infrastructure. In recent years, cyberspace has become a rapidly heightened attack landscape in warfare, and not being adequately prepared to face a cyber warfare scenario is a looming threat to the nation's prosperity. In response to the 2013 *Worldwide Threat Assessment of the US Intelligence Community*, this paper explains the importance of understanding the risks of cyber crimes and cyber espionage, how the United States government, specifically the Federal Bureau of Investigation, needs to develop a more effective strategic and tactical plan to face this threat, and how the American people need increased awareness regarding this threat through a combined partnership between the public and private sectors of the Intelligence Community.

INTRODUCTION

Cybersecurity has garnered a considerable amount of attention in the media recently as a result of increased cyber crimes and attacks in both the public and private sectors. Further, trends in cyber crime and cyber espionage suggest that more serious cyber attacks on critical infrastructures are likely to occur and that it is only a matter of time until they do. In recent years, the United States government has begun to recognize the scale and impact of the cybersecurity challenges that the nation now faces and understand that addressing these threats is necessary for the protection of the United States' economic prosperity; however, the nation is still struggling to implement an effective strategy to protect against such threats.

With new technological advances occurring every day, the cyber sphere has become a new opportunity for warfare, and cyber crimes will only increase and become more sophisticated in the wake of the ever-changing threat landscape. In order to protect the security of the United States, the government, specifically the Federal Bureau of Investigation (FBI), must work together in partnership with other members of the Intelligence Community to understand the risk of cyber crimes, develop a more effective strategy to face this threat, and provide increased awareness to the American people of how to guard intellectual property and identity in both the public and private sectors.

WORLDWIDE THREAT ASSESSMENT OF THE U.S. INTELLIGENCE COMMUNITY

The 2013 *Worldwide Threat Assessment of the US Intelligence Community* issued by James Clapper, Director of National Intelligence, examines "how quickly and radically the world—and our threat environment—are changing" (p. 1). Further, Clapper stresses the promotion of expert collaboration in all fields within the Intelligence Community (Cilluffo, 2013). In his report, Clapper (2013) identifies several threats to the United States' national security: cyber; terrorism and transnational organized crime; WMD proliferation; counterintelligence; counterspace; natural resources; health and pandemic threats; and mass atrocities.

In regard to cyber threats, Clapper (2013) identifies an increased amount of cyber attacks by both non-state and state actors that provide a heightened risk to the critical infrastructure. While terrorists and transnational organized crime organizations are behind a number of cyber threats, Clapper (2013) also identifies the non-cyber threats posed by such organizations. As the global jihadist movement decentralizes, the risk of al-Qaeda attacks on U.S. soil increases, as does the prevalence of homegrown extremists and affiliates of this terrorist group. Clapper (2013) also notes the threat posed by transnational organized crime as evidenced by drug and human trafficking, money laundering, environmental crime, and corruption. Further, Clapper (2013) cites weapons of mass destruction (WMD) as a threat to the security of the United States as more nation-states, specifically Iran, North Korea, and Syria, are obtaining or developing chemical and biological warfare-related materials for use against adversaries.

While espionage is utilized within the cyber sphere, it is also employed by foreign intelligence services, terrorist groups, transnational crime organizations, and other non-state actors to "target and acquire our national security information, undermine our economic and technological advantages, and seek to influence our national policies and processes covertly" (Clapper, 2013, p. 8). Clapper (2013) sees counterintelligence operations as a threat to U.S. government supply chains. The consolidation of infrastructure suppliers will also increase the impact of potential supply chain conversions. Distinct from counterintelligence, counterspace is limited to other nations' pursuit of capabilities to destroy the United States' access to space services, such as China's antisatellite test in 2007. Clapper (2013) believes that such threats to the U.S. space domain will increase during the next decade.

Other identified threats concern competition with regard to natural resources. Clapper (2013) states that many countries relied upon by the United States are vulnerable to natural resource shocks, such as extreme weather events, risks to water supplies, and climate change; any of these events can result in food-supply disruptions. In addition, monopolies on minerals (China) and high oil prices (Middle East) will affect the United States' ability to acquire resources. The final risks that Clapper (2013) identifies in his report on worldwide threats concern health and pandemic threats and mass atrocities. Both of these threats will continue to put humans into vulnerable situations, and will, unfortunately, be recurring features of the global landscape.

While this threat assessment offers a comprehensive and informative overview of the threats to U.S. national security, a strategic plan or roadmap for addressing and mitigating these threats is critically needed for the protection of the national infrastructure.

CYBER CRIMES AND CYBER ESPIONAGE

In the *Worldwide Threat Assessment,* Clapper (2013) states, "the world is applying digital technologies faster than our ability to understand the security implications and mitigate potential risks" (p. 1). In recent years, the threat to cybersecurity has garnered much attention in the media, including high-profile attacks on corporations including Sony, Lockheed Martin, and Citigroup (Dowdy, 2012). These current events demonstrate the inevitability that computer hackers will soon turn their targets to national security outlets (Geers, 2010). However, public understanding of the extent of damage inflicted and the cost of damage incurred as a result of cyber crime and cyber espionage is limited due to lack of

data available in the field. According to a cybersecurity expert at McAfee, less than 1% of cyber attacks that are discovered are actually reported (as cited in Dowdy, 2012). To put the potential economic impact of cyber attacks into perspective, it is worth noting that intellectual property and internet-based, e-commerce are two major drivers of the United States' economic growth, with 45 to 75% of individual companies' capital coming from their intellectual property rights (Dowdy, 2012). Cyber attacks threaten both of these realms.

The impact of cyber threats varies in intensity from small-scale, yet potentially damaging, cyber attacks on private organizations to large-scale, extensive hacking activity against the United States. A cyber attack is defined as "a non-kinetic offensive operation intended to create physical effects or to manipulate, disrupt, or delete data" (Clapper, 2013, p. 1). The types of cyber threats come in many forms, including cyber espionage. Cyber espionage is obtaining secrets without the permission of the data owner and refers to "intrusions into networks to access sensitive diplomatic, military, or economic information" (p. 1). This is typically accomplished by the use of malicious software or spyware being unknowingly installed and run on a target computer or server. Government agencies around the world have publicly noted threats of cyber espionage in recent years (Geers, 2010).

The perpetrators of such attacks range from nation-states, domestic and foreign terrorist organizations, and homegrown hackers (Cilluffo, 2013). Among the non-state actors behind cyber attacks are terrorist organizations, hacktivists, and cybercriminals. Terrorist organizations have increased interests in developing cyber attack capabilities, but these interests may be compromised by their organizational limitations and commitments to other priorities (Clapper, 2013). Hacktivists, on the other hand, continue to target companies and organizations but have not shown significant increases in their capabilities or intentions; hacktivists will target an organization, yet their interest will wane when another opportunity becomes more readily available (Salane, 2013). Cyber criminals tend to identify easy targets, as their resources are limited, yet they are a threat to U.S. economic interests through the selling of products on the black market that may enable access to critical infrastructures (Clapper, 2013).

Unlike in physical warfare, the distance between the attackers and the victims is irrelevant in cyber attacks, thus creating a bigger threat that is more difficult to both identify and prevent. The goals of cyber warfare, however, are the same: "inflicting painful, asymmetric damage on an adversary from a distance—similar to those of aerial bombardment, submarine warfare, special operations forces, and assassins" (Geers, 2010, p. 126). Yet, with cyber warfare, the attacker always has the advantage; for this reason, defenders of cybersecurity must recognize that attacks can come from anywhere in the world and they must be adequately prepared (Geers, 2010).

The threat of cyber attacks has a scope much broader than the civilian and corporate realms; in recent years, as more critical national infrastructures are becoming computerized, the fear of computer network attacks on government agencies and organizations has become a risk to the nation's security. According to Geers (2010):

> The urgency with which the FBI views the threat from cyberspace should no longer be surprising: information systems, including client and server computers, databases, and the networks that connect them are now used to facilitate the management of myriad government infrastructures. Many of these…provide the basic services necessary for the functioning of a modern society. (p. 124)

Due to the pervasive nature of this threat, the government is not only responsible for its own assets, but is also responsible for the cyber protection of the private sector as well.

President Obama launched a legislative proposal in which he declared that "threats to cyberspace pose one of the most serious economic and national security challenges of the 21st century for the United States and our allies" (Dowdy, 2012, p. 129). The key threats, according to Dowdy (2012), target the

critical national infrastructure, the government's classified information, and the intellectual property of the private enterprise. Further, in his State of the Union address, Obama expressed concern over the exposure of national critical infrastructures on the Internet, stating that "enemies of the U.S. are seeking the ability to sabotage our power grids, financial institutions, and air traffic control systems" (as qtd. in Salane, 2013, p. 1).

STATE-SPONSORED HACKERS

Nations are also utilizing the Internet for cyber espionage and intellectual property theft. This poses a significant threat, as individual organizations are not equipped with the proper resources to counter state-sponsored attacks (Salane, 2013). The United States' most threatening adversaries in the cyber domain are referred to as Advanced Persistent Threats (APT) and include China, Russia, and Iran, amongst other nations. Director of National Intelligence James Clapper identified China and Russia as "advanced" cyber actors (Cilluffo, 2013, p. 8). Each country's cyber threats to our nation are classified according to their capability and intent, including the Computer Network Exploitation (CNE)—traditional, economic, and industrial espionage, Computer Network Attack (CNA)—activities that alter targeted data and information, and Intelligence Preparation of the Battlefield (IPB) threats. Russia and China currently rank highest in both capability and intent, with Iran a close second in terms of intent, and North Korea lower on the radar in both classifications (Cilluffo, 2013). According to Cilluffo (2013), the only difference between China and Russia is that China has been caught.

China

China's sophisticated cyber espionage capabilities and impressive number of cyber attacks "appear to be intended to amass data and secrets…that will support and further the country's economic growth, scientific and technological capabilities, military power, etc.—all with an eye to securing strategic advantage in relation to competitor countries and adversaries," including the United States (Cilluffo, 2013, p. 7). One cyber espionage unit, APT1, which originates from the Shanghai region of China, conducted one of the largest state sponsored cyber attacks in recent years. According to a report released by Mandiant in 2013, APT1 maintains over 900 command and control servers in 13 countries and has conducted attacks on over 150 organizations during the past seven years (Salane, 2013). The APT1 cyber espionage unit employed a packet transmission tool to enable communication between command and control servers.

This technique was also utilized by another Chinese hacker organization, which was responsible for obtaining information that compromised RSA's SecureID Token—a device frequently used by organizations worldwide to provide secure authentication. It was later confirmed that the compromised tokens were implicated in the breach of systems of defense contractor Lockheed Martin. The primary interest of Chinese hacker organizations has been related to state-sponsored cyber espionage; China continues to be a threat to our nation as the country continues to develop more sophisticated cyber warfare tactics and capabilities (Salane, 2013).

Russia

Despite the visibility of China's cyber attacks, Russia's cyber espionage capabilities are, perhaps, even more sophisticated than those of China. Russia's extensive attacks on the United States, especially in regard to our nation's research and development, have resulted in Russia being named "a national long-term strategic threat" by the Office of the U.S. National Counterintelligence Executive (Cilluffo, 2013, p. 9). As recently as March 2013, Russian hackers released personal information about current and former United States government officials, including the Vice President and the Director of the FBI. Cyber crime perpetrators have been instrumental in increasing Russia's global crime market to $2.3 billion. These cyber attackers are comprised of patriotic hackers and organized crime organizations with assistance from

government handlers and the Russian Intelligence Service; however, Russia denies official involvement in cyber espionage-related events (Cilluffo, 2013).

Iran

Iran has been currently investing in its cyber warfare expansion through the purchase of capabilities, malware, and weapons. Unlike Russia, Iran has openly recruited hackers, such as the Iranian political/criminal hacker group Ashiyane, through the nation's Revolutionary Guard Corps. Similarly, hacker organization Basij has been hired to execute cyber espionage work on behalf of this regime (Cilluffo, 2013). Since August 2012, Iranian cyber espionage unit Izz ad-Din al –Qassam Cyber Fighters have been engaged in powerful DDoS (denial of service) attacks on financial institutions, targeting bank servers and injecting infected applications (Salane, 2013). *The Wall Street Journal* reported "an intensifying Iranian campaign of cyber attacks against American financial institutions including Bank of America, PNC Financial Services Group, Sun Trust Banks, Inc., and BB&T Corp." (Cilluffo, 2013, p. 11). Based on recent activity of Iranian cyber espionage organizations, the Los Angeles Police Department has elevated the government of Iran to a Tier One threat (Cilluffo, 2013).

THE ROLE OF THE FBI IN PROTECTING AGAINST CYBER CRIMES AND CYBER ESPIONAGE

In President Bush's 2003 National Strategy to Secure Cyberspace, he identified the Department of Justice and the Federal Bureau of Investigation (FBI) as the two government agencies given the responsibility of leading the nationwide effort to investigate and counter cyber crimes (Federal Bureau of Investigation [FBI], n. d.). The FBI, however, has a dual role in that it is expected to "prevent harm to national security as the nation's domestic intelligence agency" and "enforce laws as the nation's principal law-enforcing agency" (FBI, n. d.). Because of this double responsibility, the FBI is able to handle cybersecurity threats to the nation that stem from any source, whether from nation-states, terrorist organizations, or criminal enterprises. According to Geers (2010), the FBI's current top three priorities are preventing terrorist attacks and high technology crimes (which include cyber attacks), and maintaining foreign intelligence operations. The FBI partners with other members of the U.S. Intelligence Community to collaborate on strategies and tactics to use in preventing and responding to the growing threat of cyber attacks on the nation.

The FBI leads the National Cyber Investigative Joint Task Force (NCIJTF), which is located in Washington, D.C. and is the national focal point for conducting cyber threat investigations. The FBI also supports the Department of Homeland Security's mission by "investigating threats and incidents which affect the security of protected computers and networks" (FBI, n. d.). Using a multi-disciplinary approach of the entire homeland security enterprise working together, actions taken by the FBI have been successful in preventing and dismantling cyber threats:

> The FBI's capacity to respond to cyber incidents and emergencies in communities nationwide is enhanced through task force partnerships with other law enforcement agencies. Key federal, state, and local cyber investigative and forensic personnel, sworn and civilian, are teamed together in this endeavor. The FBI is enhancing the capabilities of each of its cyber task forces to address the full range of cybersecurity threats and function as extensions of the NCIJTF. No other agency can match this broad and robust presence, which is crucial for timely and effective incident response. (FBI, n. d.)

This idea of developing partnerships includes ongoing collaborations between the government and the private sectors, including affected industries, security researchers, and academia. The FBI also partners with the National Cyber Forensics and Training Alliance (NCFTA) through which the agency is able to share intelligence (FBI, n. d.).

To further increase the levels of communication between the public and private sectors, the FBI established the Internet Crime Complaint Center (IC3), in partnership with the National White Collar Crime Center (NW3C), "as a means to receive cyber crime complaints from consumers and businesses for action by authorities, and to disseminate fraud alerts to the public" (FBI, n. d.). In addition, the FBI oversees a team of cyber experts from a variety of information technology backgrounds who are dedicated to serving the public by addressing cyber concerns and penalizing those who victimize the American people through the force of cyber attacks.

One example of the FBI's efforts in investigating and responding to cybercrimes is evident in the Operation Ghost Click mission, a two-year FBI investigation that led to the arrest of six Estonian nationals who ran a sophisticated Internet fraud ring that infected and dismantled approximately four million computers in more than 100 countries. The perpetrators were also able to obtain close to $14 million through corrupt Internet advertising schemes. Further, they defaced legitimate corporations throughout their scheme; for example, when targeted users clicked on the link for iTunes, they were instead taken to a website for a business unaffiliated with Apple that claimed to sell official Apple software, thus defaming the corporation. For this reason, the total cost incurred as a result of this attack is far greater than the $14 million dollars directly received by the attackers; like other cyber attacks, the incurred damages are immeasurable (FBI, 2011).

RECOMMENDATIONS

Despite the extensive progress made in response to the ever-changing threat landscape, the United States, specifically the government agency of the FBI, can and should assess and respond to cyber threats more effectively. The goal should be to maintain good crisis management. Government agencies, especially the FBI, should seek partnerships, specifically through international collaborative initiatives, in an effort to more effectively counter "the transnational nature of cyber attacks" (Geers, 2010, p. 129). Most critical to these collaborative efforts is the partnership of the public and private sectors to prevent major cyber threats.

The government needs to promote the emerging "security-economic complex," in an effort to bolster defense capabilities in the wake of potentially harmful cyber threats. To accomplish this, "policymakers should drive private enterprise to protect its intellectual property adequately…supporting the security-economic complex to develop into a fully functioning system in which the economic incentives of private enterprise and cybersecurity vendors align with government's incentive to protect long-term prosperity" (Dowdy, 2012, p. 140). There are four key elements to the security-economic complex approach, which include: increasing the accountability of the government in regard to the protection of intellectual property in the public and private sectors; implementing an incentive program for the private sector and cybersecurity vendors to generate further involvement in research and development for threat prevention; ensuring that relevant information is effectively and efficiently communicated to private sector stakeholders so that they are better equipped with the intelligence they need to prepare for, respond to, and recover from a security threat; and creating a roadmap and information-sharing platform for stakeholders to share experiences of past attacks in an effort to prevent future ones (Geers, 2010).

By placing intellectual property protection on the government's public agenda, policymakers will play an active role in ensuring that the threat to cybersecurity is as low-risk as possible. To do so, policy changes are necessary in two areas. First, policymakers should employ best practices to "ensure that details held by security agencies on the extent of the cyber threat are shared with elected officials and hence ensure that knowledge on the extent of the threat to intellectual property is well understood across governments" (Geers, p. 140). Second, through increased communication, more information on the extent of the cyber threat should be shared "to incentivize private enterprise to invest in management and technology to protect intellectual property" (p. 140). In creating new policies, questions concerning the following topics should be considered: what best practices can

be established for public and private interagency information sharing regarding threat intelligence; what role the government should play in assisting the private sector in threat identification; what government guidelines should be implemented for private sector incident reporting; and what framework the government can establish to ensure the private sector maintains the technical ability to respond to a cyber attack (Geers, 2010).

Further, the United States government must also work closely with companies to ensure that there are consequences for the perpetrators who commit cyber attacks that breach private defenses (Cilluffo, 2013).

CONCLUSION

The Internet "is merely a large collection of networks managed by different nations, companies, universities and telecommunications companies throughout the world"; however, the key to keeping a global Internet functioning relies on "the mutual and self-interest of the players" (Salane, 2013, p. 4). These "players," or stakeholders, must utilize this global network positively in ways that will mutually benefit themselves and others. When this sense of communal trust is lost—as seen through cyber attacks and espionage events—"a global, open, free Internet, along with many of the benefits it offers, may turn out to be a short-lived part of history" (p. 4). The threat of cyber-related attacks will not disappear in future years; in fact, if no action is taken to prepare and address these threats, attacks will continue to increase at the expense of our national security.

One of the largest vehicles for continued economic growth and prosperity is the expanding cyberspace infrastructure. Protecting that infrastructure is a much-needed investment that the FBI, other government agencies, and the private sector should focus on by working collectively to create partnerships that meet the demands of the constantly evolving cyber threat landscape and its relation to our critical national infrastructure.

REFERENCES CITED

Cilluffo, F. J. (2013, March 20). Cyber threats from China, Russia, and Iran: Protecting American critical infrastructure. *Homeland Security Policy Institute: The George Washington University.* Retrieved from http://www.gwumc.edu/hspi/policy/Meehan_Cilluffo Testimony March 2013.pdf

Clapper, J. R. (2013, March 12). Worldwide threat assessment of the US Intelligence Community. *Senate Select Committee on Intelligence.* Retrieved from http://www.intelligence.senate.gov/130312/clapper.pdf

Dowdy, J. (2012). The cybersecurity threat to U.S. growth and prosperity. In N. Burns & J. Price (Eds.), *Securing cyberspace: A new domain for national security* (1st ed.), (pp. 129–143). New York: The Aspen Institute.

Federal Bureau of Investigation. (n. d.) Addressing threats to the nation's cybersecurity. *The FBI: Federal Bureau of Investigation.* Retrieved from http://www.fbi.gov/about-us/investigate/cyber/addressing-threats-to-the-nations-cybersecurity-1

Federal Bureau of Investigation. (2011). Operation ghost click: International cyber ring that infected millions of computers dismantled. *The FBI: Federal Bureau of Investigation.* Retrieved from http://www.fbi.gov/news/stories/2011/november/malware_ 110911/malware_110911

Geers, K. (2010). The cyber threat to national critical infrastructures: Beyond theory. *Journal of Digital Forensic Practice,* 3, 124–130. doi: 10.1080/15567281.2010.536735

Salane, D. E. (2013, March 21). The looming threats of cyber war and cyber espionage. *The Crime Report.* Retrieved from http://www.thecrimereport.org

AUTHORS

Brian Lozada (blozada1@gmail.com) is the director of information security at Abacus Group, a provider of hosted IT solutions for hedge funds and private equity funds. He is responsible for the development and maintenance of Abacus's information security program. Prior to joining Abacus Group, Lozada was the director of information security at Condé Nast and has held senior technology and information security positions at Sony Music Entertainment, Vonage and Accenture. Lozada is CISSP certified and has a BS in information security. He is currently completing his MS in homeland security at Monmouth University.

Making the Community Project Approach Work in Your Community

Denise M. Pheils, PhD

ABSTRACT

A problem facing many new cybersecurity graduates is how to find a position working in the cybersecurity field without experience. One way to make the classroom relevant, provide hands-on cybersecurity experience for graduates to list on their resume, and provide value to the community is through the community project approach to cybersecurity courses. The community project approach involves service at not-for-profit organizations applying a security solution to an existing problem, such as an unsecured wireless network or writing a disaster recovery plan for the organization. By applying the concepts and techniques learned in class, students learn relevance and application of areas of study, as well as build confidence. This work builds on a previous article and presentation and provides specific information to replicate the activities in the reader's own community. Concepts covered include identifying not-for-profit organizations with which to partner, identifying appropriate projects for specific courses, structuring the student teams, troubleshooting issues in the field, and applying a more generic rubric to ensure equity and consistency in grading. This case study includes lessons learned in the field and comments shared from evaluation forms and letters. Use of the community project approach improves student skills and understanding while providing a necessary service for a not-for-profit organization and helping to secure each community, one organization at a time.

INTRODUCTION

Cybersecurity is a field dominated by 'experience required' positions (Cybersecurity Jobs Report, 2013). The need to provide experience for students and workers new to the field is difficult when most positions require previous experience. This creates a cycle wherein the experience necessary to qualify for a position can only be gained if one already has the necessary experience to get the position. While this conundrum exists in many fields, it is more noticeable in cybersecurity as the field is much younger than most other information technology (IT) and information systems (IS) positions. Creating a means to provide relevant, practical experience for students who do not take an internship or cooperative course/work experience is difficult. The problem of needing the experience prior to acquiring a position that will provide necessary experience for cybersecurity positions is also faced by those who have been downsized out of positions in the IT and IS fields and are now competing with new graduates and other displaced workers. If a position is not found quickly, information technology (IT) and security skills become dated. What follows is a practical guide to maintaining timely skills and relevant application of those skills, as well as a way to provide proof of those efforts in a practical way on the resume or curriculum vitae while benefiting the community and showing volunteerism.

The community project approach is detailed in the ACM InfoSec Curriculum Development Conference Proceedings (2013). Briefly stated, however, it is a method of instruction where students are exposed to real-world problems at not-for-profit (NFP) organizations to allow for problem solving, planning

and solution implementation, project management, interpersonal skill enhancement, improved self-efficacy and community improvement (Pheils, 2013). Organizations in need of assistance are identified and students complete the work under the supervision and direction of the instructor. Upon completion of the project(s) students are presented letters on the organizations' letterhead thanking them for their efforts and detailing some of the work completed. The letters serve as poof of their efforts and to support entries students may make on their resumes highlighting the skills used and the specific tools and techniques demonstrated. NFP organizations benefit by receiving solutions to issues in the form of volunteerism and community support. Artifacts including the completed work project and the letter of appreciation allow students to move from learner to practitioner (Grant & Branch, 2005). Students apply concepts to real-world, unscripted situations, practice professionalism, and gain a better understanding of information technology and security industries and jobs. Connecting course content to problems students will face in the business environment are necessary elements for what Lavoie and Rosman term 'successful education.' Faculty have a variety of experiences to help them stay current with technological advances and application, a dynamic 'classroom' environment, unique problems to solve, and relevant and timely issues to study.

The community project approach is a method of applying practical experience to information technology and security courses through andragogical principles (Knowles, 1980) and volunteerism in the community. This approach was employed in order to identify needs for students to gain hands-on experience, adopt course content including relevant and timely material, and assist students in building confidence and enhacing their resumes (Knowles, 1980). The community project approach is based on project-based learning and meets the standards identified by Thomas (2000) as the approach is based in constructivism, student teams determine the solution, the project is the main focus of the class, application of the main course concepts is central to learning. In addition, and as the projects are based on needs of community organizations they meet the criteria of providing a realistic project.

This approach has been employed successfully for several years and in several communities by associate-level, bachelor-level, and certificate-seeking students. In addition to the solutions provided to organizations, this approach provided students an increased interest in the courses, satisfaction in their learning, self-efficacy, and a feeling of well-being from assisting the organizations, as reported in end-of-class surveys.

Lavoie and Rosman (2007) determined education to be made up of two factors: effective teaching, where effectiveness is demonstrated in student understanding and application; and a strong curriculum. Deschryver, Leahy, Koehler, and Wolf noted the need to consider the impact of rapid technological change on our instruction and educational settings (2013).The community project approach offers active teaching and learning environments supported by curricula that assume a holistic approach to IT and security topics as none are isolated in practice. With the workplace as the classroom the ability to show and adapt technology is provided.

The use of a project as the focus of teaching segments is founded in constructivist methods for teaching and learning. With the focus on a continuing project, the basis or 'story' for the application of course concepts and techniques is known and becomes comfortable and less of the focus than the actual problem identification, solution formulation, and application. The project is the framework or scenario introduced to the class and becomes the basis for problem identification, troubleshooting, appropriate tool and technology selection, project management, evaluation of various options, and ultimately installation, configuration, and use of equipment and programming solutions.

While the focus of this article is to aid teachers in building community projects into their courses, there is practical advice and material that can be used if the reader is out of work or wishes to enhance or strengthen a skill set. The method may also apply

to faculty who wish to maintain a current skillset with real-world practice and application. Herein, we detail the use of a course to complete a community project, however, the same idea may be applied for a single person or a small team of faculty seeking hands-on experience to provide greater insight into the dynamic IT and IS fields during a classroom experience. Topic areas are clearly delineated and worded for different audiences to identify specific areas of interest within the article.

HOW TO FIND NOT-FOR-PROFIT (NFP) ORGANIZATIONS IN NEED OF ASSISTANCE

One of the most daunting issues to address when using the community project approach is identification of viable projects at willing organizations. The good news is that once successful work has been completed for an organization it is very likely that word will spread and organizations will begin to contact you. The main source of opportunities for the community project approach is through NFPs due to their philanthropic missions and their constant need for assistance and perpetual lack of funding. NFPs are usually set up for volunteer workers, simplifying the process of a class or individual going into the organization to provide assistance. Specific departments within a college campus may be able to provide names of organizations looking for assistance or may be willing to pass on contact information if an inquiry is made. These departments include the main switchboard or operator, jobs or placement offices, marketing media or outreach offices, and the specific disciplines where the courses are listed such as the School of Business or the School of Engineering.

Often members of the class have affiliations with organizations, or faculty have served on community boards and committees and have contacts with directors or employees. The local Chamber of Commerce may be able to provide names of local organizations seeking assistance; e.g. NFPs aiding the elderly or providing shelter and counseling for victims of battery and abuse. Many organizations have newsletters or websites that may list 'Help Wanted' sections or 'Call for Action' areas. In addition to funds, stationary supplies, and canned goods, several NFPs to-do list include items such as painting and cleaning assistance, website development or maintenance, training on a specific software application, etc. Such specific information also provides an idea of what platform and applications the organization may use in their service of the community. The easiest way to approach an organization is to treat this as a networking opportunity and let everyone know that you are seeking an organization in need of assistance with solving an IT problem. When all else fails, simply looking through the phone book may provide leads to purse through cold calls by the teacher or the class.

While the focus has been on NFP organizations this does not mean that these are the only organizations available or viable for projects. With for-profits the process is similar. When considering a request for assistance the business may be considered for its contribution to the school or institution, including a history of hiring students. Several for-profit small businesses were assisted because of their hiring history and commitment to sponsoring events and other school endeavors. When assisting small businesses the approach is similar to NFP as there is no charge for services. The classes and teachers provided the expertise and labor; any equipment needed was usually purchased by the business or NFP; and, in a few instances, donations were acquired on behalf of the NFP.

MATCHING PROJECTS WITH CLASSES

Identifying organizations to partner with is only part of the planning process. Determining the appropriate scope and scale of each project within the organization is another important factor. An understanding by NFP and selected small businesses is that there may be a delay in the class actually completing the work. Most institutions offer a variety of courses each term but not necessarily the same courses every term. Planning for current and future courses requires an understanding of the curriculum and specific course objectives. Creating network cables may not be an effective project for a network security course, but if that task is only a

small part of a larger project, it may be a perfect fit. A necessary part of information security education is the need to approach security holistically and not as a silo. Marquardt and Waddill (2004) warn of compartmentalizing learning theories and content into silos as it is unrealistic and denies the student a real-world approach.

A project that demonstrates the breadth of skills necessary may provide students with a realistic view of what will be expected when they are employed. An organization may need more assistance than they realize and suggestions may lead to an appropriately sized project. This is common when organizations are offered a safety and security assessment and a disaster recovery (DR) plan. Most NFPs encountered in this project do not have a DR plan in place but would quickly benefit from one as it shows their commitment to continuing and future planning. In addition, a partial plan (absent confidential information) can be included with or noted in grant applications. Grant-funded organizations may benefit from this documentation since 'long-term vision' and 'sustainability' are key areas in grant writing (Davis, 2005, p.2).

It can be difficult to find a project located close enough to the school and available during course time. The logistics of transportation and course time and the availability of the necessary personal at the facility and avoidance of peak hours or sensitive situations can be complicated. One facility for battered women and children would not allow any men onsite. Such situations call for creativity in the planning process. The teacher may need to take on more of a physical role in visiting the facility, taking photos, relaying information, and aiding in planning the project off-site. Other opportunities may include paring cross-class teams so students who are available to go to the site may serve in that capacity and those unable to attend may work as remote consultants. If acceptable to the organization, technology can be used to include all students and participants through video calls such as Skype and Google Hangouts; asynchronous discussions facilitated through the school's online Learning management System (LMS); texts and photo sharing; shared resources and content via the LMS, Google Docs, or services like DropBox.

As word of the hands-on, real-world projects spread throughout the institutions, students began to expect that such projects would be available for certain courses every term. That expectation alleviated the need to 'sell' students on how wonderful it would be to complete a real-world project instead of a case study or teacher-created, scripted project (Pheils, 2013). An alternative 'hands-off' project is always available, but to date, with over 50 successfully completed projects, no student has opted for this alternative.

STRUCTURING STUDENT TEAMS

Application of the community project approach has included arrangements for most projects prior to the beginning of a course. The difficulty with preplanning is that the project is suited to the course content and identified course outcomes, but not necessarily to the students enrolled in the course. As with most educational environments the make-up of courses is dynamic and varied and the same course taught each term will not have students with the exact same strengths and skill sets.

To facilitate a workplace experience, students are provided an overview of the course, syllabus, real world project, and alternative project during the initial course meeting. Students are asked to prepare or update their resumes (removing address and phone number) and to be prepared to interview for positions during the next class period. In the second class meeting, the instructor has listed teams and job positions specific to the planned project on the board without any student names. The highest position requiring the strongest skill set is the project manager for each team. The instructor selects each project manager based on 'interviews' in front of the class with students who desire that position. The instructor then adds to each team the project scribe who will document each step, record individual assignments and progress, and work as the 'right hand person' or assistant to the project manager.

The project scribe for each team is usually a student with limited IT or security skills who would often be selected towards the end of the team selections. This alleviates the stress many students have of being the last person selected, provides the project lead with a named assistant, and usually provides a spirit of inclusion when building teams. Next, the project managers begin to build their teams by selecting students based on their skill set and the needs of the project. The teacher acts as moderator to ensure no team has students with significantly stronger skill sets than other teams. If the project is of a larger scope it may be preferable to select teams to target specific project activities or focus areas, such as a hardware team, a software team, and a team to develop training and resource reference materials (this latter team will aid the organization in utilizing the solution once the course has been completed).

Students are informed of the potential to earn awards for their contributions and the criteria for such awards. The project focus is on contribution and personal growth, not beginning skills. Since the class is meant to provide the necessary skills, if a student already possessed such skills, there would be no criteria with which to gauge mastery and learning of the course material. The focus on resumes and potential awards usually removes the favoritism aspect of selecting teams. Most project managers select teams of high achieving students based on grades or understanding (even if this means not selecting a friend). The additional benefit to the students is that their up-to-date resumes will allow them to apply more quickly when a job opportunity is identified.

TROUBLESHOOTING ISSUES IN THE FIELD

An area that may cause faculty unease, when considering the community project approach, is the issue of what to do if a problem arises when the class is in the field. Real-world problems are not scripted and, therefore, are hard to anticipate or solve quickly. Part of the real-world experience is the possibility that the unexpected can occur. Part of the instructor skill set must include flexibility, humility, a broad understanding and application of the topic, and a willingness to use such issues as teaching opportunities. Several successful projects included 'Internet Scavenger Hunts' to identify unknown information. With a real-world project, an assumption may not be enough to use as a basis for a decision, and using the issue as an opportunity to conduct research and identify if the assumption is probable or if another possibility is correct benefits students. It is the rare employee who never has to ask a question, seek advice, or weigh possible outcomes before making a decision. Showing students how to handle uncertainty shows the strength of the instructor's skill set as it is impossible to know everything about a subject. When in doubt, it is advised to select projects that are well within the faculty's knowledge and experience base.

It may be necessary to settle disputes or change team population if severe conflict occurs. Allowing teams to first manage their own conflicts is often beneficial for the team and each member's personal growth. A study by Stone and Bailey (2007) suggests that allowing teams to self-resolve issues builds student self-efficacy. Serious conflicts may need to be addressed in the field, quickly, quietly, and with as little disruption as possible. Taking the time to build teams and observe the interactions among all members may provide insight as to which teams may have problems and allows for reorganization prior to leaving the classroom.

CREATING AND APPLYING A RUBRIC FOR GRADING AND OUTCOME ASSESSMENT

Courses employing the community project approach will probably not accommodate traditional grading and scoring methods. The focus of these courses is on proof-of-concept, communication skills, professionalism, team work, and growth of the individual. To appropriately quantify and qualify student achievement against course outcomes and successful completion of the project a custom rubric is used. While authors have noted that teachers and the literature are not consistent in what a rubric is or how it should be used (Leist, Woolwine, & Bays, 2012; Wenzlaff, Fager, &

Coleman, 1999), Lund (2000) identifies a rubric as a tool for evaluating student work based on a pre-described set of standards and criteria.

The rubric should be sufficiently vague to allow for application to each course without major renovation for differing projects, courses, and terms. Reed (2008) authored the paper "No Rubric Can Describe Magic' to stress the need to allow for creativity in assessment. Creativity is usually assessed in technology courses (West, Williams, & Williams, 2013) and should be added to any rubric used for the community project approach as much of the success of a team and of the project is the application and use of creativity. West, et al, (2013), suggest that an infusion of creativity in all facets of problem-based learning enhances ideas and that technology may actually inspire creativity.

As the content of each course is specific to the course outcomes and objectives, it may be beneficial to develop several rubrics to accommodate different situations or to make the rubric general so as to apply to all applications. Gallo (2004) notes that rubrics should be designed before the project begins and rubrics should be shared with students early in the process so they are aware of what they will be assessed against.

Creation of multiple rubrics to allow for variations in projects may be beneficial; equally beneficial is the use of multiple rubrics to assess different parts of the project, keeping the assessment items simple and straight forward. Gallo (2004) notes issues with one rubric that attempts to capture all aspects of an assessment as being too 'challenging' for most teachers and he advocates the use of multiple rubrics to address specific areas of the work. Lund (2000), notes that rubrics are essential to aligning what is assessed with the instructional process.

The PACE approach to rubric design inspired many of the rubrics used in community project-applied courses (Tufte, 2005). The actual rubric presented in Tufte's (2005) paper is not applicable, but the major topics assessed, including participation, appearance, cleanup, engineering, and safety, are part of the rubrics created for the courses. The areas have been changed or extended, like the appearance category that includes appearance and evaluates cleanliness, neatness, adherence to the casual dress code for visiting the sites, and includes politeness, courtesy, and respect.

LESSONS LEARNED IN THE FIELD

A self-assessment may be beneficial prior to using a community-based project in a course. Live problems and the uncertainty of a different environment can be stressful. It is possible that the instructor will not know the answer to a problem immediately. Humility is a beneficial trait that eases stressful and unknown situations. Proper preparation of the class for the unexpected and unknown environment may dispel unease.

The 'audience' aspect of a live project can serve to place students on their best behavior, or it can cause anxiety due to lack of confidence in one's skills. A lesson learned in the field is that students behave differently in and out of the classroom. The quiet, reserved student may become the boisterous team member, while a student who appears to always have the answer in a classroom setting may become introverted when visiting the NFP organization.

A plan for conflict resolution is beneficial, as is taking time to specify clear and distinct expectations for behavior and interactions with the staff of the NFP. For example, it is helpful to establish that only the instructor may commit the class to any work or activity for the NFP. A pre-class visit by the faculty prior to taking students to the cite provides information on the space, the overall project, if the students' work will be in front of patrons or 'behind the scenes,' and the general working conditions.

The most significant 'take-aways' from the past several years include: 'expect the unexpected'; prepare a sound plan for solving the NFPs problem; define expectations for each site visit prior to leaving the classroom; have extra paper and pens for documenting information; and receive prior approval from administration. Prior to embarking on the first community project approval from administration

was secured, but additional legal documents were needed including release of liability for the NFP and the school, non-disclosure forms and attendance sign-in sheets to document the attendance of students on-site.

STUDENT COMMENTS AND CRITIQUES

Prior to beginning any project, students are offered a choice of the community project or a traditional case study to complete in-class (Pheils, 2013). Most student comments compared the recent experience with past courses. While all comments had positive information, a few mentioned preferences in team members and many were simply one word comments such as "Great!" or "Best class yet." The following are a few student comments from course evaluations:

> "This was the best class ever!"
>
> "We need more classes to finish the rest of the work they [the NFP] need done. I want to audit the next course so I can help with the next part."
>
> "We need more time to work as a team. This was a great experience."
>
> "I never knew my teacher knew so much. She knew what to do and not because the book said to."
>
> "I wish [the NFP] was open at night so we could keep working."

THE NEXT STEP

The community project approach has successfully been applied to single on-ground courses, online courses, and cross-class teams (where the teams consist of students from the online course section and the on-ground section of the same course). The approach has been successful in several different communities in three states (Indiana, Ohio, and Michigan). Additional constraints have been applied, such as no males allowed at one of the battered women's shelters. This required the female students to complete all of the hands-on work and the male students to work as consultants and gather quality research to support their efforts.

One area of application not yet attempted is to apply cross-school teams allowing associate or bachelor degree-seeking students to partner with students in another geographic area or in a graduate IT or security program. Another area of application would be to pair IT and security students with students from different (non-IT and security) disciplines. Schaffer, Chen, Zhu, and Oakes (2012) advocate cross-disciplinary teams as potentially more effective at problem solving than teams constructed from students of a single discipline. Working with cross-school or cross-discipline teams would require additional effort to construct an appropriate rubric to accurately capture the contributions and efforts of all team members.

CONCLUSION

The community-based project approach to teaching IT and security classes has been effective for several years in different communities in three states. Application of the approach provides students a timely, relevant, and effective venue for application of the concepts learned in class which support constructivist, andragogical (Knowles, 1980), and project-based learning (Savage, Chen, & Vanasupa, 2007). The use of team-based and self-directed learning through research and application may increase student self-efficacy. Students challenged to research beyond classroom content may aid in creating life-long learners (Savage, Chen, & Vabasupa, 2007).

Partnering with area NFPs benefits the community and the students who completed the project. Students who experience the community project approach may have an increased interest in their coursework and an increased satisfaction in their accomplishments. Building their resume with volunteerism and practical work training may provide students with enough practical experience to earn an interview for IT or security jobs. Learning is a process requiring active participation on the part of the student to be

truly effective (Savage, Chen, & Vabasupa, 2007). Application of course topics elevates students from listeners to researchers and practitioners.

The community project approach is not a one-size-fits-all solution for all programs, schools, or courses. It may not be the best situation for all students. The information in this paper is presented to offer an alternative to traditional, or static, coursework that may provide an opportunity for students to become engaged in their learning and in their communities.

REFERENCES CITED

Cybersecurity Jobs Report (2013). The Abell Foundation and CyberPoint International, LLC. Retrieved from http://www.ctic-baltimore.com/reports/Cyber%20Security%20Jobs%20Report-010813.pdf

Davis, B. (2005). Writing a Successful Grant Proposal. Minnesota Council on Foundations MCF Reprint Series. Retrieved from http://www.mcf.org/system/article_resources/0000/0325/writingagrantproposal.pdf

Deschryver, M. D., Leahy, S. M., Koehler, M. J., & Wolf, L. G. (2013). The habits of mind necessary to generate new ways of teaching in a career of constant change. *TechTrends, 57*(3), 40-46. doi:http://dx.doi.org/10.1007/s11528-013-0661-1

Gallo, A. M. (2004). 5 simple steps to designing a rubric. *Strategies, 17*(5), 21-24. Retrieved from http://search.proquest.com/docview/214546330?accountid=42681

Grant, M. M., & Branch, R. M. (2005). Project-based learning in a middle school: Tracing abilities through the artifacts of learning. **Journal of Research on Technology in Education, 38**(1), 65–98.

Knowles, M.S. (1980). *The modern practice of adult education: From pedagogy to andragogy.* (2nd ed.). New York: Cambridge Books.

Lavoie, D., & Rosman, A. J. (2007). Using active student-centered learning-based instructional design to develop faculty and improve course design, delivery, and evaluation. *Issues in Accounting Education, 22*(1), 105–118.

Leist, C. W., Woolwine, M. A., & Bays, C. L. (2012). The effects of using a critical thinking scoring rubric to assess undergraduate students' reading skills. *Journal of College Reading and Learning, 43*(1), 31–58. Retrieved from http://search.proquest.com/docview/1373205285?accountid=42681

Lund, J. L. (2000). Creating rubrics for physical education. Assessment series K–12 physical education: National standards for physical education a guide to content and assessment. St. Louis: Mosby.

Marquardt, M. J. & Waddill, D. (2004). The power of learning in action learning: A conceptual analysis of how the five schools of adult learning theories are incorporated within the practice of action learning. *Action Learning Research and Practice,* 1(2), 406–429.

Pheils, D. M. (2013). Applying a community project spproach to IT and security courses. Proceedings from ACM InfoSec Curriculum Development Conference 2013. Kennesaw, GA: ACM.

Reed, Y. (2008). No rubric can describe the magic: Multimodal designs and assessment challenges in a postgraduate course for English teachers. *English Teaching, 7*(3), 26. Retrieved from http://search.proquest.com/docview/926191882?accountid=42681

Savage, R. N., Chen, K. C., & Vanasupa, L. (2007). Integrating project-based learning throughout the undergraduate engineering curriculum. *Journal of STEM Education, Innovations and Research, 8*(3), 15–27. Retrieved from http://search.proquest.com/docview/222790217?accountid=42681

Schaffer, S. P., Chen, X., Zhu, X., & Oakes, W. C. (2012). Self-efficacy for cross-disciplinary learning in project-based teams. *Journal of Engineering Education, 101*(1), 82–94. Retrieved from http://search.proquest.com/docview/1014006072?accountid=42681

Thomas, J. W. (2000). A review of PBL. Retrieved from http://www.bie.org/research/study/review_of_project_based_learning_2000/

Tufte, Robert B.,Jr. (2005). The P.A.C.E.S. grading rubric: Creating a student-owned assessment tool for projects. *The Technology Teacher, 64*(5), 21-22. Retrieved from http://search.proquest.com/docview/235290584?accountid=42681

Wenzlaff, T. L., Fager, J. J., & Coleman, M. J. (1999). What is a rubric? Do practitioners and the literature agree? *Contemporary Education, 70*(4), 41. Retrieved from http://search.proquest.com/docview/233033616?accountid=42681

West, R. E., Williams, G. S., & Williams, D. D. (2013). Improving problem-based learning in creative communities through effective group evaluation. *Interdisciplinary Journal of Problem-based Learning, 7*(2).

AUTHOR

Denise M. Pheils (denisepheils@gmail.com) earned her PhD in education specializing in Online Teaching and Training from Capella University. Her training in IT includes an MBA in information systems of management and a BBA in management information systems and 21 professional certifications, including the Certified Information System Security Professional (CISSP) and Project Management Professional (PMP). Prior to entering academia, Pheils was an analyst for several national and global companies in a career spanning 19 years. Pheils is adjunct faculty for Excelsior College and faculty for Texas A&M University Commerce. She was a professor at Owens Community College for

almost 15 years. During that time she developed many courses, including the core System Security and Information Assurance degree courses; she also mapped the content to the NSA's 4011 & 4012 curriculum standards, and sought and was awarded the NSA's accreditation of the Center of Academic Excellence for Two-Year Schools (CAE2Y). Pheils is on the board of directors for the Northwest Ohio Infragard Chapter and several college and secondary school advisory boards. Pheils was 2010 Teacher of the Year for ACBSP region 4 and serves as a section editor for the *Journal of Digital Forensics Security and Law*.


EXCELSIOR COLLEGE
FOUNDED IN 1971