Open Access License Notice

A Mission Assurance Paradigm for Cyber Competition

Abstract – Current incarnations of cyber competitions emphasize network attack and defense over information assurance. Capturing or defending network assets represents an end, rather than a means to accomplish a broader mission. In this paper we present a cyber competition paradigm focused on assuring a mission. Consistent with traditional engineering competitions, competitors bring their own designed artifacts to the competition to fulfill their assigned mission. Our competition focuses on assuring orders transmitted across a cloud computing environment. We present a framework for the implementation of an assurance based competition and demonstrate the competition through a digital chess game. We distinguish our competition from existing models by awarding points for success in a competition domain distinct from, but coupled to cyberspace.

Index Terms – Information Assurance, Security, Cyber Competition

I. INTRODUCTION

Technological advances in the last decade coupled with the availability of internet services has transformed cyberspace into a pervasive domain connecting users across spatial, temporal, and organizational boundaries. We conceive cyberspace as "*...a global domain within the information environment consisting of the interdependent network information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers,"* [1] and recognize the intrinsic interconnectedness of the cyber domain.

The empowerment provided by cyberspace to civilian and military organizations comes with a cost, as cyberspace has become a distinct, vulnerable center of gravity of these organizations [2]. Unfortunately, a 2011 Bloomberg Government Survey indicates that 172 Fortune 500 companies spent $5.3 billion a year and estimate they thwart 69% of cyber attacks. Even if their collective spending were to increase to $46.6 billion the companies estimate they could only foil 95% of cyber attacks [3]. The projected national shortfall of cybersecurity professionals compounds the problem. Even if organizations decided to improve their cyber defense posture, it is unlikely these efforts could be appropriately staffed [4].

Efforts to increase the number of cyber security professionals are important, but address only half the problem. The reality is that traditional computer science and engineering curriculums focus on the creation of reliable systems in permissive environments that fail at first contact in a contested environment [5].

Spafford noted the same pattern in [6], observing "*...basic skills such as how to write secure, resilient programs and how to protect information privacy are not included in standard courses but relegated to the elective course."* Integrating cyber competition into existing curriculum provides students a means to learn both how to create secure systems and appreciate the consequences of failing to do so [7, 8].

[α] *Research Engineer*
[β] *Research Engineer*
[γ] *Research Engineer*
[δ] *Computer Engineer*

II. CYBER COMPETITION

The DEFCON 4 capture the flag (CTF) competition in 1996 established the first generation of publically hosted large scale cyber attack competitions [9]. Consistent with the notion *"...that the offense outpaces the defense, and the offense is better than the defense,"* [10] the emergence of cyber defense exercises integrated into the educational curriculum occurred five years later with the Cyber Defense Exercise (CDX) [11]. The growing cyber threat has since prompted the integration of cyber attack and defense competitions into civilian graduate programs [12], undergraduate education [7, 13], and high school enrichment programs [14].

Although cyber competitions include elements of coding challenges [15], reverse engineering competitions [16], exploit creation contests [17], and digital forensic investigations [18], we consider network centric competitions in this paper. Network centric competitions include implementation specific variations, but we broadly classify current cyber competitions as a combination of capture the flag, king of the hill, and attack/defend-the-network. We differentiate our assurance based cyber competition paradigm from existing models in Section B after describing these four paradigms in Section A.

A. CYBER COMPETITION PARADIGMS

CDX has established itself among the most well known defensive cyber competitions. With an emphasis on assuring the availability of services, CDX fits the defend-the-network paradigm. An additional challenge for CDX competitors includes designing a network using open source security components that can provide a predefined set of critical services [11]. Before competition begins, a dedicated attack team composed of industry experts inspect the proposed networks, implant vulnerabilities into the systems, and approve them for competition. To score points competitors must keep their services running in the face of a coordinated attack by an invited red team.

Where the CDX competition defines the attack surface by requiring the inclusion of implants, services, or operating systems, attack the network events invite competitors to attempt to exploit vulnerable network targets. Although attack/defend-the-network competitions are often merged [19], in its pure form attack-the-network rewards competitors for establishing a presence on the network, disrupting critical services, and the exfiltration of information.

The attack-the-network label provides a general description for exploit based competitions. Competition organizers have created events that emphasize remote exploitation [20], and two notable specializations exist within the attack paradigm: king of the hill and capture the flag. In both cases the attack-the-network framework establishes the competition space as a set of predefined systems defined by competition organizers. Organizers may encourage competitors to disrupt, deny, deceive, degrade, and destroy systems of their, but the benefits of these attacks are indirect. To score points in king of the hill competitions, competitors maintain a persistent presence on the target systems [21]. To claim a system, competitors generally announce their presence to competition organizers and competitors by changing the banners of one or more of the system services.

In contrast with king of the hill, capture the flag competitions require competitors to retrieve cyber artifacts from their targets. Capture the flag (CTF) focuses on information exfiltration but requires the exercise of a broad range of exploitation tools. At the UCSB International Capture the Flag event organizers deploy static targets for competitors to capture [20]. Other competitions require competitors to also host and protect flags on their own system.. For example, the DEFCON CTF requires competitors to both host targets with vulnerable services and to steal the flags of their adversaries [19].

Capture the flag competitions distinguish themselves from other competitions by emphasizing the importance of protecting information. Other competition variants conflate defending or attacking networks with assuring information. Across all four competition types, protecting information or a network represents a goal in and of itself rather than a means to generate effects in the physical domain.

The first large scale integration of effect generation in a separate battle space occurred with the 2011 Shmoocon Hack Fortress competition [22]. We propose a tighter coupling between information assurance and generating effects in the natural world through a mission assurance paradigm for cyber defense. We develop the relationship between mission assurance and cyberspace in the next section.

B. Mission Assurance

Across civilian and military organizations, establishing assured systems and processes is a key component to mission success. Techniques through which organizations strive for assurance include failure modes and effects analysis, redundancy, and Six Sigma. Collectively, assuring the systems and processes that compose an organization represents an approach to assure the mission of the organization. In this paper, we define a mission as *"The task, together with the purpose, that clearly indicates the action to be taken..."* [23]. We use the term mission to describe the activities of an organization and recognize that the goal of assurance techniques is to define *"...a process to ensure that assigned tasks or duties can be performed in accordance with the intended purpose or plan,"* [24].

Missions conducted in and through cyberspace inherently include information operations. The set of information operations performed by a cyber system include generation, processing, storage, communication, consumption, and destruction [5]. To assure a mission through cyberspace, it is necessary to assure the constituent information operations that compose the mission. In a broad sense, mission and information assurance are identical in cyberspace. Both guarantee the confidentiality, integrity, and availability of information by assuring the operations that compose a mission.

Information assurance represents a divergent approach from network security/defense methodss used to assure cyber missions. The assumption that protecting network infrastructure enables control over all information operations underlies network security/defense. Although successful defense can protect information, it does not represent a necessary condition for mission assurance. Defending a network to protect information is analogous to defending the entire ocean to protect a ship.

In contrast, the foundation for information assurance is in the creation of systems and architectures that innately provide the confidentiality, integrity, and availability necessary to complete a mission. To assure these properties, our competition required competitors to create their own software implementations. Competitors demonstrate assurance properties of their systems using formal methods and machine verified proofs [25]. Formal methods provide a sound basis for competitors to specify their trust assumptions, identify protected resources and establish access control policies. We discuss the integration of mission assurance concepts into the structure of our competition in the next section.

III. Cloud Captures Queen

Cloud Captures Queen (CCQ) reflects the duality of cyberspace as an enabling and operating domain [26]. During CCQ each competing team uses a cloud with a customized software implementation to pass messages to an operator in their battleground, a digital chess game. Chess provides a historical precedent in higher education and a rich strategic backdrop for CCQ. In traditional chess, an opponent cannot disrupt the choice of a move and its execution. CCQ splits the move choice and execution between spatially disparate command and execution teams who form an ad hoc coalition for the game. We refer to the command team as the CMDR and the execution team as the OPR in this paper. The CMDR issues orders, while the OPR executes the orders and informs the CMDR which move the opposing coalition made.

As an operating domain, teams attempt to generate effects in cyberspace that directly affect the orders or situational awareness of their adversary while assuring their own operations. We describe the supporting network infrastructure for CCQ in Section B and the game server in Section C. First, we outline the general competition structure in Section A.

A. Competition Structure

CCQ requires the participation of at least four competing teams and a neutral white team. The white team takes responsibility for operating the overall game server, scoring server and defining the network

structure that includes routers, switches, and server hardware. Competitors bring their software implementation, written in the programming language of their choice, to the competition. Figure 1 outlines the required pathway for message passing and distinguishes between teams and coalitions.

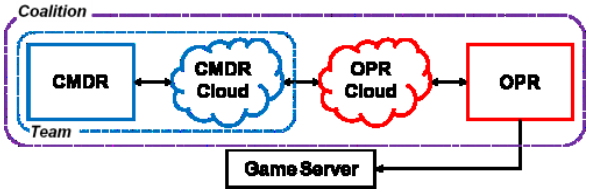

Figure 1: CCQ Coalition Structure

The collaborative element of the competition illustrated in Figure 1 requires ad hoc coalitions to interoperate with one another. To facilitate interoperation we require teams to submit their source code to the other teams a week before the competition. The competition aspect of CCQ provides the opportunity to craft exploits when the team belongs to an opposing coalition.

In CCQ, teams simultaneously join multiple coalitions and act as both CMDR and OPR for different coalitions. These roles require teams to perform four concurrent tasks during the competition: (1) issue orders for chess piece movement to their OPR, (2) execute orders of their CMDR, (3) report the status of the battlefield to their CMDR, and (4) initiate attacks on the enemy coalition.

Prior to the initiation of competition, the white team provides each team with a competition factsheet that specifies when they can access a battlefield, the location in cyberspace of the battlefield, and their role in the battle. Figure 2 shows an excerpt from a competition factsheet.

```
3.2.2/SIMULTANEOUS ENGAGEMENTS ARE REQUIRED//
3.2.3/BATTLESPACE INTERNET PROTOCOL ADDRESS IS 192.168.1.240//
3.2.4/IDENTIFICATION INITIATION CODE/MA/DESMOULINS//SB/URBANII//
3.3/PHASING/IMPLEMENT OFFENSIVE OPERATIONS IAW THE FOLLOWING SCHEDULE//
3.3.1/081630ZAUG2012/DEPLOYMENT OF FORCES IAW STANDARD CHESS FORMAT//
3.3.2/081700ZAUG2012/STANDARD CHESS FORMAT/C2-MA/EX-SB//
3.3.2.1/COMMPLAN/PORT 1863//
```

Figure 2: Competition Factsheet

In Figure 2 line 3.2.3 specifies the battlefield and line 3.2.4 assigns two teams named MA and SB specific codes to establish themselves as the CMDR and OPR respectively. Figure 2 also specifies the engagement start time, the start location for the chess pieces, and the required connection port. To begin a battle, the white team spawns a battlefield through the instantiation of a game server. The game server waits for the competing OPR teams to connect. Failure to connect by the OPR results in an automatic loss for that coalition. Commands sent to the game server require 128 bit Advanced Encryption Standard (AES) with Cipher Block Chaining for semantic security [27].

Before the white team launches a game server, a separate key generation server uses a Diffie-Hellman exchange to derive an AES key for the CMDR. The CMDR can share this key with the OPR to bypass message passing, but doing so endangers the CMDR battlefields that have different OPR's. Figure 3 shows the Diffie-Hellman and Encryption tabs of the CCQ cryptography client provided to all teams.

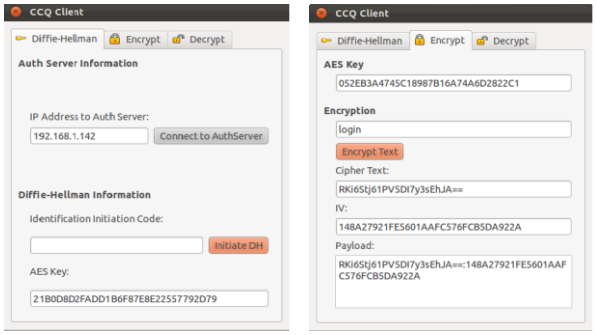

Figure 3: CCQ Cryptography Client

The white team provides the internet protocol (IP) address needed for the Diffie-Hellman tab in Figure 3 as part of the competition factsheet. The server side of the Diffie-Hellman client in Figure 3 stores the generated AES key locally for the white team to load into the game server. For the CMDR, the client in Figure 3 facilitates key management by automatically adding the key to the encrypt/decrypt tabs of the client. The encrypted payload from the encrypt client includes the initialization vector with a "*::*" delimiter and base 64 encoding.

The CMDR possesses the keys to interact with the game server while the OPR possesses the ability to connect to the server. To play a game, commands must pass through the CMDR and OPR implementations. Games begin with a race to connect and seize the initiative by playing as white. The CMDR begins submitting orders to the OPR team to upload to the battlefield through the CCQ Communication Client shown in Figure 4.

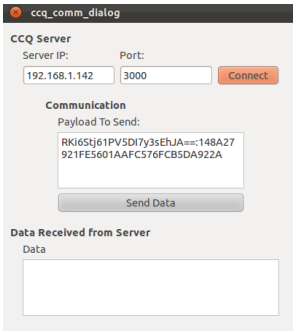

Figure 4: Encrypted Login

Through the CCQ Communication client the OPR submits encrypted orders to the server. Each coalition has a four minute time limit to specify a move. Failure to submit a move means the server makes a random move on behalf of the player. Part of the OPR responsibility includes sending the move of the opposing coalition to the CMDR. Without this intelligence, and careful tracking of the adversary, the fog of competition quickly obscures the battlefield.

To earn points in CCQ, coalitions must capture enemy pieces or secure the battlefield by checkmating their opponents. Scoring follows the standard chess piece point distribution [28]. A checkmate results in a full point distribution to the winning team. A separate scoring server provides real time score updates to teams and spectators. While individual hacks themselves do not score points, efforts to disrupt, deny, deceive, degrade, or destroy the enemy team can reap rewards across multiple battlefields. To enforce adherence to the competition structure outlined in this section we created a specific supporting network architecture discussed in the next section.

B. Supporting Network Architecture

To create a realistic and challenging cyber exercise, the network architecture must enable the goals and inherently enforce the rules of the exercise. We designed the network to provide control and flexibility to the white team and to mold the landscape for successful game play for each team. We held the exercise in a facility with a large conference room and smaller adjoining meeting rooms that did not have cellular access. The facility allowed us to physically separate the teams. The teams had to rely on their implementations to establish communication and publish/execute their chess moves through their C2 systems. The following diagram depicts the network architecture by subnet and desired traffic flow.

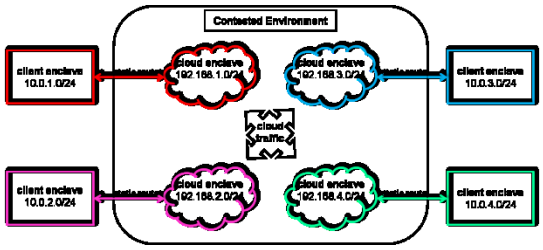

Figure 5: CCQ Network Architecture

An important design goal for the exercise was to utilize the network architecture to enforce access control, traffic flow, and competition rules. We did not want to introduce any "artificial" rules into the exercise. For example, it would be a poor design to build a flat network and then have the white team declare and enforce a soft rule for "no ARP spoofing."

The network architecture and technology that surrounds the exercise must enforce the exercise objectives. The router acted as the backbone of our network architecture. We chose to use a standard server with the Ubuntu Server operating system as our custom router. We installed a network interface for each LAN on our network and enabled traffic forwarding in Ubuntu. Each individual network interface acted as the gateway for one of the subnets in the network. This provided us the advantage to create and use IPtable rules to enforce our traffic objectives. By manipulating the FORWARD chain in IPtables we created the rules for each client enclave that permitted access to their cloud enclave only. Each enclave operated within a private subnet and firewall rules allowed client enclaves to access only their cloud implementations.

Anyone on the white team with Linux and networking experience could administer the server without facing a substantial learning curve. We used Etherape to visualize the network during the exercise and presented the network on a large monitor to show visitors network traffic and effects generated by competing teams during the exercise [29].

We could also use different networking programs to visualize, monitor, and present the traffic in different representations for the white team and scoring team. We utilized private IP address ranges with dnsmasq to provide DHCP and DNS. Finally, we collected all the exercise traffic for post-exercise analysis and lessons learned.

C. Game Server Design

Our server design assumes teams can attack the white servers to affect the battle space. This assumption influences the secure design and coding of the game and key servers. Our server console can spawn an arbitrary number of game servers to increase the size of the competition. Each game server implements multi-threaded sockets to prevent deadlock of connections and limits the number of simultaneous connections to two, one for each OPR. The game server authenticates OPR connections using the encrypted login command in Table 1. The game servers operate as state machines that define the behavior of network processing. Figure 6 describes the four game server states, and the requirements for state transition.

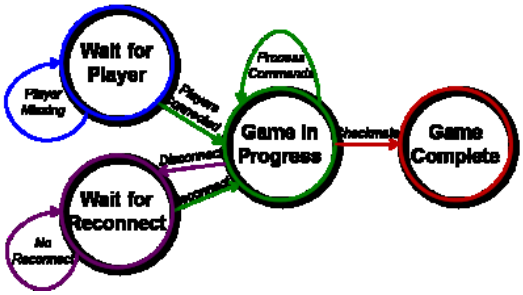

Figure 6: State Diagram for Game Server

The states in Figure 6 represent the entire flow of a game. The OPR connections dictate all transitions except Game Complete. To control the state transitions, the game server subjects all inputs to stringent data parsing that allows the server to assess payloads and eliminate the threat of crafted malicious packets. The game server contains a set of regular expressions to differentiate between commands. The server does not provide any response to commands that contain invalid notations. Table 1 demonstrates an example command, the corresponding notation, and an example server response.

Table 1: Move Notation

COMMAND	NOTATION	RESPONSE
Move piece from e2 to e4	m_e2_e4	Move success!
King side castle	m_O-O	Move success!
Queen side castle	m_O-O-O	Move success!
Request square a8	r_a8	BR (Black Rook)
Last move	lastmove	m_e7_e5
Game info	info	57000 ms
Status	status	GAME IN PROGRESS

IV. CCQ EXERCISE

The inaugural CCQ included four separate teams composing two static coalitions composed of seven members. Static coalitions provided a stable basis for the competitors and enabled the white team to more efficiently administer the event. The CMDR and OPR teams of a coalition communicated their chess moves using a symmetric key known only to the CMDR. With static coalitions, a risk exists that the CMDR could bypass their implementations by sharing their symmetric key with the OPR. We implemented a soft rule to prevent sharing and monitored teams for our competition. In the remainder of this section we discuss the natural fog and friction of CCQ in Section B, the results in Section C but first summarize the competition structure in the next section.

A. COMPETITION STRUCTURE

The coalition composition included computer scientists, mathematicians and computer/electrical engineers. The individual teams kept their own self determined names, and we named the two coalitions the *Rebel Alliance* and *Galactic Empire*.

A week before the CCQ competition the white team provisioned each team with the following competition supplies: 4x Dell Elitebook 8560w with Windows 7, 1 TB external hard drive, Dell Precision T7500 server tower, local network infrastructure, Backtrack 5, CCQ Crypto Client, CCQ Comm Client, command list to interact with the server, competition factsheet, and source code to opposing coalition implementations.

The competition factsheet included eight engagements over a three hour period with an escalating frequency as the competition progressed. The aggressive schedule design replicated the stress inherent to assuring real cyber operations. Further, it tested the leadership abilities of the teams and their ability to establish an effective organizational structure. The physical separation of the coalition combined with a challenging schedule of engagements produced the desired effect across the coalitions in taxing their ability to act as CMDR, OPR, and cyber warriors.

B. COMPETITION RESULTS

Restricting teams to communication through their implementations presented communication barriers that made it difficult for the CMDR to possess perfect battlefield knowledge. The physical separation of coalition members necessitated stable lines of communication for information to pass from the CMDR to the OPR and on to the game server. Difficulties with communication lead to issues with tracking games and frustration within coalitions.

Competition participants did not encounter difficulties disseminating and submitting movement orders during the first scheduled game. Lack of physical interaction constrained all communication to the cloud infrastructure. Both coalitions encountered difficulties as the second game launched. The introduction of another engagement required teams to act as both CMDR and OPR for the separate games. The increasing responsibility forced teams to keep track of movements and make movement decisions in one game while monitoring the cyber environment for orders to submit to the game server for another game.

The ability to communicate effectively allowed the *Rebel Alliance* to overcome the escalating responsibility that comes with executing multiple simultaneous chess games. The *Rebel Alliance* was able to maintain reliable and secure lines of communication. This provided the members of that coalition a way to communicate with each other and operate effectively in both games. Stress and confusion affected the *Galactic Empire* with the introduction of the second game. The *Rebel Alliance* used the confusion and stress brought on by a second game to launch a successful attack against their adversary and exploit an implementation-level vulnerability. The exploit kept ports used in communication in a half-open state that degraded communication between the members of the *Galactic Empire*. The *Rebel Alliance* was initially unaware of the success of their exploit and proceeded cautiously throughout the remaining engagements.

The *Galactic Empire* did not immediately discover the attack. The stress of multiple engagements coupled with no apparent feedback from teammates facilitated a breakdown in the coalition dynamic. The degradation of communication prevented members from quickly troubleshooting difficulties and discovering the source of the disruption. The disorientation experienced by the *Galactic Empire* created difficulty in tracking the ongoing engagements. The degraded communication, stress, escalating responsibilities and quickly deteriorating coalition cohesion prevented the *Galactic Empire* from recovering until the end of the competition. Figure 7 summarizes the competition scores at the end of the competition.

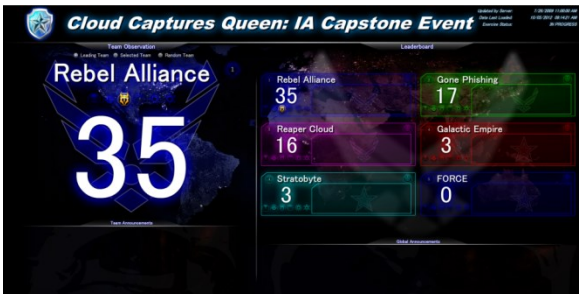

Figure 7: CCQ Scoring Server

Both coalitions and event observers had access to the web page shown in Figure 7 to monitor the competition score. The disparity in the score reflects the organizational and technical superiority of the *Rebel Alliance* coalition. The success of the *Rebel Alliance* rests on the pillars of clear communication between the CMDR and OPR, establishment of clear responsibilities, and execution of a timely attack. The *Galactic Empire* struggled primarily due to their focus on detecting the exploit, reacting to the exploit and recovering. The confusion sown by the successful *Rebel Alliance* attacks forced the *Galactic Empire* to cede six of the eight scheduled chess games.

V. CONCLUSION

In this paper, we examine the current structure of cyber competitions in the context of mission assurance. We recognize that civilian and military organizations assure their systems and processes to accomplish the set of missions that they have defined as necessary for their success. Current cyber competitions do not provide a strong link between successful cyber operations and a successful mission for their organization. Instead, competitions with a defensive emphasis focus on maintaining service uptime and resolving pre-existing vulnerabilities. Defending the network becomes the mission, rather than a means to accomplish a larger task. Attack-the-Network exercises like king of the hill and capture the flag

emphasize system exploitation but do not link successful exploits to completing a mission. In both cases, attack/defend-the-network competitions award points for a successful exploit. Further, defensive competitions require participants to patch together defenses for intrinsically vulnerable systems and do not encourage the construction of initially secure solutions.

In contrast with current attack/defend-the-network paradigms, the Cloud Captures Queen competition reward competitors for successfully creating secure implementations. CCQ rewards attacks indirectly, as successful attackers gain the opportunity to exert greater influence over their battlefield. Instead of emphasizing traditional defensive measure, CCQ encourages teams to focus on the cyber assurance aspects of a software implementation they bring to the competition. Competitors established a basis for assurance through formal methods and automated theorem provers. CCQ provided the opportunity to test their implementations in a realistic, contested environment.

The competition provided competitors a chance to learn how to manage communication styles, assign roles/responsibilities, and the importance of technical preparedness before the competition. CCQ requires teams to coordinate a chess game with an unfamiliar group across a contested environment. Many teams quickly learned how to establish communication channels once they lost track of their chess boards. Moving cloud implementations into a different facility and network environment required planning and expertise of the system. Teams learned that each member must have enough knowledge in all facets of their implementation to guarantee success.

In a cyber competition, the planning, logistics, and schedule are as important as the underlying technical features and architecture. We must improve on communicating the purpose and requirements of the exercise, provide the competitors with enough information to become familiar with the exercise environment, and execute chess games in a more automated and fluid fashion.

For future capstone exercises, we plan to make the following improvements: implement dynamic coalitions, standardize the cloud architecture for each team, coordinate with the teams more effectively to allow for more preparation time leading up to the competition, and include the traditional attack and defend assets into the competition framework. Standardization of the cloud implementations enable teams to spend additional time developing automation and working with the design and verification of their implementations.

VI. ACKNOWLEDGEMENTS

This research was supported by the U.S. Air Force Research Laboratory/Information Directorate. All opinions expressed in this paper are the authors and do not reflect the official policy or position of the Air Force Research Laboratory, the United States Air Force, Department of Defense, or the United States Government.

VII. REFERENCES

[1] Director for Operational Plans, 2009, *Joint Publication 1, Doctrine for the Armed Forces of the United States*, Department of Defense, Washington, D.C.

[2] Rattray, G.J., 2001, *Strategic Warfare in Cybersapce*, United States of America: The MIT Press.

[3] Garfinkel, S., 2011, "Inside Risks: The Cybersecurity Risk," *Viewpoints*, Association for Computing Machinery: Communications of the ACM. **55**(6), pp. 29 - 32.

[4] Finkle, J., Randewich, N., 2012, "Experts Warn of Shortage of U.S. Cyber Pros," Reuters.

[5] Jabbour, K., Muccio, S., 2011, "The Science of Mission Assurance," *Journal of Strategic Security*, **4**(2), pp. 61-74.

[6] Spafford, E.H., 2009, "Cyber Security: Assessing Our Vulnerabilities and Developing an Effective Defense," *Lecture Notes in Computer Science*, **5661**, pp. 20 - 33.

[7] Conklin, A., 2006, "Cyber Defense Competitions and Information Security Education: An Active Learning Solution for a Capstone Course," *Conference on System Scuences,* Kauai, HI.

[8] Mullins, B.E., Lacey, T.H., Mills, R.F., Trechter, J.M., 2007, "How the Cyber Defense Exercise Shaped an Information-Assurance Curriculum," *IEEE Security & Privacy*, **5**(5), pp. 40 - 49.

[9] Gavas, E., Memon, N., 2012, "Winning Cybersecurity One Challenge at a Time," *IEEE Computer and Reliability Societies*, **10**(4), pp. 75 - 79.
[10] Barrett, D., 2012, "U.S. Outgunned in a Hacker War," *Wall Street Journal,* 28 March, http://online.wsj.com.
[11] Schepens, W.J., 2003, "Architecture of a Cyber Defense Competition," *IEEE International Conference on Systems, Man and Cybernetics* Washington, D.C.
[12] Gunsch, G.H., 2003, "Integrating CDX into the Graduate Program," *IEEE International Conference on Systems, Man and Cybernetics,* Washington, D.C.
[13] Carlin, A., Manson, D., Zhu, J., 2008, "Developing the Cyber Defenders of Tomorrow with Regional Collegiate Cyber Defense Competitions," *Information Systems Educators Conference*, Education Special Interest Group of AITP, Phoenix, AZ.
[14 White, G.B., Williams, D., Harrison, K., 2010, "The CyberPatriot National High School Cyber Defense Competition." *IEEE Security & Privacy*, **8**(5), pp. 59 - 61.
[15] Poucher, B., 2012, "Giving Students the Competitive Edge," *Communications of the ACM*, **55**(8), pp. 5.
[16] Internet, 2012, *CSAW CyberSecurity Competition*, [cited 2013 Jan 31].
[17] Internet, 2012, *Pwn2own Competition*, [cited 2013 Jan 31].
[18] Lacey, T.H., Peterson, G.L., Mills, R.F., 2009, "The Enhancement of Graduate Digital Forensics Education via the DC3 Digital Forensics Challenge," *42nd Hawaii International Conference on System Sciences*, 10.1109/HICSS.2009.433, Honolulu, HI.
[19] Cowan, C., Arnold, S., Beattie, S., Wright, C., Viega, J., 2003, "Defcon Capture the Flag: Defending Vulnerable Code from Intense Attack," *Proceedings of the DARPA Information Survivability Conference and Exposition*, 10.1109/DISCEX.2003.1194878, Washington, D.C.
[20] Childers, N., et al., 2010, "Organizing Large Scale Hacking Competitions," *Detection of Intrusions and Malware, and Vulnerability Assessment*, editors Kreibich, C., Jahnke, M., **6201**, Berlin/Heidelberg, Springer.
[21] Science Applications International Corporation, 2012, "SAIC CyberNEXS King of the Hill," [cited 2013 Jan 23].
[22] Conti, G., Babbitt, T., Nelson, J., 2011, "Hacking Competitions and Their Untapped Potential for Security Education," *IEEE Security and Privacy*, **9**(3), pp. 56 - 59.
[23] Joint Chiefs of Staff, 2011, *Department of Defense Dictionary of Military and Associated Terms*, Department of Defense, Washington, D.C.
[24] Lynn, W.J., 2012, *DOD Policy and Responsibilities for Critical Infrastructure*, Department of Defense, Washington, D.C.
[25] Chin, S.-K., Devendorf, E., Mucio, S., Older, S., Royer, J., 2012, "Formal Verification for Mission Assurance in Cyberspace: Education, Tools and Results," *Colloquium for Information Systems and Security Education*, Lake Buena Vista, FL.
[26] Jabbour, K., 2009, "The Science and Technology of Cyber Operations," *High Frontier*, **5**(3), pp. 11 - 15.
[27] Goldwasser, S., Micali, S., 1984, "Probabilistic Encryption," *Journal of Computer Systems*, **28**(2): pp. 270 - 299.
[28] Capablanca, J.P., Firmian, N., 2006, "Relative Value of the Pieces," *Chess Fundamentals*, Random House, New York, NY. p. 24.
[29] Internet. 2012, *EtherApe: A Graphical Network Monitor*. 2012 [cited Jan 23, 2013].