# A Cyber Security Multi Agency Collaboration for Rapid Response That Uses AGILE Methods on an Education Infrastructure

Erik Moore, Dan Likarish

Regis University, Center for Information Assurance Studies, Denver, Colorado, USA
emoore@regis.edu, dlikaris@regis.edu

**Abstract.** This study provides a summary and analysis of a cyber security multi agency collaboration for rapid response by Regis University (RU), in partnership with the Colorado Army and Air Force National Guard (CONG) and the State of Colorado (SOC), deploying AGILE methods to improve the ability of the CONG and SOC to respond to attacks against Colorado's critical infrastructure. The summary covers formative discussions and about a year-long series of physical exercises, lectures and certification exams that advanced the study participants domain knowledge, awareness of SOC policy and communication with industry. Other states and territories can use the model to the benefit of their citizens. Events included multiple simulations, physical exercise scenarios, and table top exercises designed to give real-world substance to more abstract cyber security concepts and integrate physical world consequences to actions performed by the participants.

**Keywords.** cyber, security, multi agency, collaboration, rapid response, agile, inter-agency, infrastructure, physical exercise, line training, Colorado, simulation, National Guard, state exercise, constraint, defense, operations, education

## 1 Introduction

Defense forces operate under highly constrained procedures because of the high impact of their work, their security requirements, and their culture of readiness. This means that training for standard operations is often formulated as standard operating procedure similar to combat *LINE Training* that is highly structured. Cyber conflict, however, operates across multiple types of government and private infrastructure administered with many types of professional practice. As different agencies move to more collaborative and agile defense postures in support of this heterogeneous cyber infrastructure, training exclusively for an independent formal style of operations might overlook significant complexity when preparing to support less structured civilian cyber infrastructure teams who are working in collaborative environments against malicious actors whose impetus may turn out to have arisen from organized crime, nation state activity, or loose collaborations of hactivists. This multiparty scenario creates a highly complex environment where agile collaboration and mutual awareness of differing

operational practices would likely be required to achieve high levels of joint capability while maintaining legal boundaries. In the context of this emerging challenge, Regis University invited the leadership of the Colorado National Guard to the Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) and perceived the value of a more open collaborative training model the RMCCDC and other Regis-hosted competitive and collaborative hands-on events. The Collegiate Cyber Defense Competition (CCDC), developed and organized by the University of San Antonio [1], is a nation-wide cyber defense competition at the college level that has steadily grown to encompass all 50 States in the Union. The approximately seven teams from different institutions are composed of eight to ten students who maintain secure digital services while defending against active cyber attacks and addressing business challenges. In 2012 Regis University joined the CCDC as the last organizational unit, the Rocky Mountain CCDC (RMCCDC) [2]. In consequence of its RMCCDC experience Regis extended the lessons learned from the RMCCDC to its lab-based online and classroom courses, professional user groups and local schools. The CONG leadership, in January 2013, observed a big training advantage in that the types of physical exercises (active scenarios using technology with challenges), tabletop events, and formal lecture training models employed at Regis were not exclusive to any sector or agency. Regis initiated the first effort to leverage this multilaterally compatible structure across agencies and civilian sectors through a successful Information Assurance Scholarship Program Capacity Building grant application submitted to the National Security Agency Education Directorate. The grant application mapped out an extensible model of collaborative capability building activities that would be applicable to the 50 United States of America and related territories. In addition, a significant number of individuals present from other national guard units and law enforcement agencies also participated.

As Steven Cooper *et al* well expressed the historical context of such efforts, [3] cybersecurity training and education evolved through a wealth of sector-specific training that has matured over the last 40 years, including the CISO-style training that matured into SANS; the information security education programs that perhaps started as early as Queensland Institute of Technology in Australia offered a Master's level research degree in computer security 1986. Cyber security forces capabilities in departments of defense around the world began to mature as evidenced by the expansion of the U.S. Air Force Mission to include cyberspace in 2005. [4] Alternately, a review of trends in cyber investigation as developed by federal and law enforcement [5] provide strong operational capabilities requirements that support the types of skills that would lead to situational awareness in support of effective response to cyber security incidents.

Regis and the other parties initiating this effort set as the primary goal to offer multiple agencies and civilian entities the opportunity to maintain relationships that enable rapid collaborative response and integrated skill development, raising the level of joint capabilities. In context, the collaborative's work extended an earlier ACM education model that places high value on a student's "working knowledge in actually using their skills to interact with the society at large."[6] Individually each participating entity in the collaboration identified their own targeted results. The Colorado National Guard (CONG) expected to leverage the differential between commercial education and

internal training to provide a broader experience. The CONG leadership also wanted to achieve a stronger socialization with state and civilian participants. The State of Colorado was expecting to extend their existing training programs and have regular skill-refresh events. Regis was hoping to improve their competition engines, and refine their AGILE-based management structure given a new and broader set of collaborative customers. In addition, Regis expected significant individual knowledge and technical capability benefits of faculty and students who participated in the event.

Regis University provided the technology that facilitated simulation, training, and tool walk-through activities. These include enterprise layer 3 switches, multi-terabyte class production storage network, blade server sets, virtual machine infrastructure, and remote console capabilities provided in team rooms. Regis provisioned this network previously for large multi-team competitive events, research sandbox environments, coursework laboratory space, and industry training events. As Regis deployed diverse configurations in support of this set of applications, the team developed an AGILE-based development and management model.

## 2 Study Methodology

This study uses case study methodology[7] generally to present and analyze the collaborative efforts from its inception and initial deployment through the current expectations one year after the first event. This study provides background information on the expected needs and describes how the partners managed operation change, developed solutions, and provide mutual review of the outcomes. This study does not provide specific data on the technical outcomes of individual performance, operational details specific to participants, or descriptions of specific technologies used in the specific simulation scenarios as based on interviews, observation, and related references. Also it presents preliminary criteria by which events like this can use for assessment, based on stakeholder objectives.

## 3 Joint Training Event Design Activities

The leaders of each participating entity contributed specific resources to the effort and exposed specific needs in January of 2013 in order to allow for a collaborative design process based on gap analysis. The Colorado National Guard brought a strong functional cyber security vision and technical security expertise while needing a customized education and a collaborative way to socialize with operations partners in both private and public sectors. The State of Colorado brought a different but overlapping cyber security expertize in addition to their functional requirements. Regis University brought an infrastructure of handling joint physical exercises, a conference facility, and a pool of staff and students to facilitate activities. Regis hoped to use this set of events as an opportunity to improve training facilities and methods, gain faculty and student experience, and further develop the AGILE methodologies that it had begun to use in support of academic computer laboratory infrastructure.

The Xmodel represented in Figure 1 indicates both the joint effort of the three initial participants and the gateway they represent to larger groups. While the State of Colorado is an exclusive entity, it could also provide this model to other states in support of their own collaborative activities.

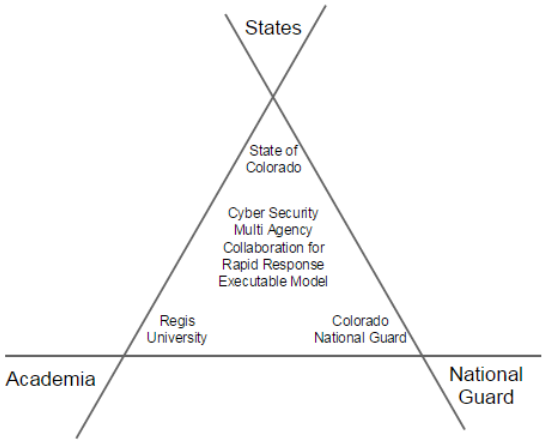


**Fig. 1.** Initial Xmodel for Collaboration and Cooperation

The collaborative used many scenarios to build the events, but the primary scenario portrayed the exhaustion of a single private sector or agency's resources and the need to have rapid and well-prepped teams to provide escalated capabilities for incident response. The "Call in the Guard" scenario breaks down into the following steps:

1) A private entity or group of entities becomes overwhelmed by a cyber security event that has scale and scope significant to the State of Colorado. The entity(s) resources are exhausted and further action is called for.
2) The private entity calls the State of Colorado to provide assistance.
3) The Governor's Office assesses the situation and escalates by calling in the Colorado National Guard to provide cyber security support as "cyber smoke jumpers."

In order for this sequence to be successful, well-interfaced lines of communications need to be pre-established and well-tested processes, plans, and roles should be invoked in a collaborative way. During the first collaborative session the leadership team realized that having more active participation from the private sector early on provided greater validation for the simulation and tabletop scenario events. Figure 2 represents the new model for interaction.

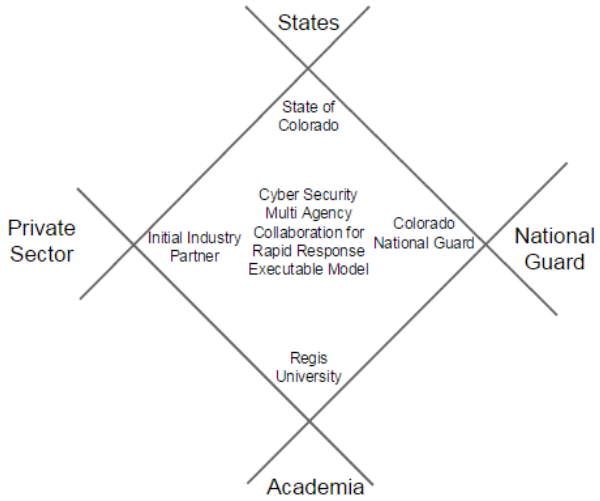


**Fig. 2.** Updated Xmodel for Collaboration and Cooperation - Includes Private Sector

To ensure the value of the event for all participants, the formative group performed gap analysis of the sum of the contributed resources in relation to what would be necessary to fulfill the expected needs of each group. The Gap analysis of resources versus needs that took place before the first collaborative event was expected to be speculative at best, and the formative team decided to employ an iterative Agile methodology that provided on-the-fly tuning during events and significant tuning of activities and resources between events.

### 3.1 **Capability Gap Analysis**

The joint leadership team focused on the gap between current joint capabilities and desired future capabilities in regards to rapid and agile joint operations as deployed with *ad hoc* civilian teams that currently protect critical infrastructure. This required that a coordinated response happen rapidly with existing civilian infrastructure teams, and that these teams all be familiar with each other. In Support of this the joint leadership team identified within their agencies a need for mutual tool awareness. Considering a higher layer of coordinated incident management, they also set as a goal the coordinated implementation of disparate policies, such that each organization understands the boundaries and professional practices of their partners.

These expected operational needs led to the development of the multi-agency collaboration. The leadership identified through gap analysis the need for a low-pressure training environment that allowed for those policy sets to be meshed in a series of response scenarios. Each group would be aware of how their agency should respond, but would develop an understanding of other agencies' practices and procedures.

### 3.2 Logistical Hurdles of Inter-agency Collaboration

As the event came closer, the collaboration leadership team discovered logistical hurdles that were artifacts of the multi-sector effort. The national guard schedule required the events be set on the weekend, while state employees needed to get credit for their time off. The technical team at Regis needed to de-provision some of the technical infrastructure from regular education labs and deploy it exclusively for the weekend virtually overnight. This multi-party coordination challenge existed partly because both the National Guard and the State of Colorado staff saw great value in having the event take place live, face to face, in a location with a minimum of distraction. The physical exercise was the hardest thing to accommodate. The facilities needed a lecture hall large enough for all participants and relatively secure rooms for the teams defending active web services.

Regis University uses a pool of volunteer faculty, students, and partners to facilitate these types of events. Therefore, the Regis Staff works hard not to overburden any individual volunteer. To respond to this issue the Regis team uses an AGILE-based method to build into each development and deployment cycle the specific load of requirements that they are able to handle in one cycle.

### 3.3 Collaborative AGILE Development Methodology

Over the past 10 years, Regis has been developing an agile process by which infrastructure is maintained and deployed using a very small staff, each with other responsibilities, and a pool of volunteers from the affiliate faculty, alumni, students, and members of the professional community. This situation required an AGILE [8] development model that accommodated a significant flux in human resources, mix of donated, loaned, and core university equipment, and manages. Te Regis team named it the Framing Forward Model, and presented it to The Colloquium in 2014. Briefly, it is composed of three layers. In the event layer teams adjust, in real-time, active cyber scenarios to navigate towards successful completion. In the middle Workspace Layer, teams work jointly on a particular project develop scenarios to prepare for events. In the lowest Services layer, the department tracks what human and technical resources are available at any one time to manage demand and allocate resources to project work-spaces. Using that model, the Regis staff and volunteers have met needs for a broad range of events like the Rocky Mountain Collegiate Cyber Defense Challenge, the Information Systems Security and Information systems Auditing and Controls Association professional development events, classroom-supporting laboratory environments, etc. This new challenge of providing cross-sector hands-on events required a new level of agility.

## 4 Timeline of Events Across First Year of Collaboration

The collaboration included several types of events along the following general timeline. Between these major events the planning team designated intermediate activites where individuals or groups could prepare for upcoming events and focus on skill development in order to enhance their technical contribution to the events. The following bulleted list provides a general timeline of events. The multi-month cycle of learning that this pace incited yielded obvious results in discussions as participants convened at the beginning of each event.

- August 2013 - Event 1 - This event focused on incident response in a red/blue team format. The big lesson learned from this event was that the exercise needed to include more contextual details of operation and success criteria in addition to a standardized technical configuration
- Intermediate time 1 - During this time participants worked on security training, with some completing CISSP and Security+ certifications.
- February 2014 - Event 2 - This event focused on cyber forensics and a review of the tools of investigation. Physical exercises included forensic challenges and vendors presented relevant products.
- Intermediate time 2 - During this time participants continued on certifications including Ethical Hacker training.
- August 2014 - Event 3 - This event contained an array of policy, socialization activities, tabletop scenarios, a physical exercise, and malware response review. By this time, participation had grown to include six state guard units, representatives from two Centers of Academic Excellence, and State of Colorado IT and public safety personnel.
- Intermediate time 3 - Participants continue external training and certification in preparation for the next collaborative event.

While the annual timeline is fairly well structured, it is not ridged in that the Regis team adapted the events in real time and debriefed after every event, in order to feed input in to the AGILE development cycle. As new needs became evident, the joint leadership used the intervening time to tune the upcoming collaborative sessions.

## 5 Joint Exercise - Collaborative Session Components

The Collaborative Leadership Team formulates each session agenda from separate components listed below. The collaboration leaders compiled this component list from pre-existing academic education activities, military exercises, and traditional training methods that each partner brought to the table. However, the content of each component varies from session to session.

- **Partner Mutual Introductions:** This fostered mutual awareness of command hierarchy, jurisdictional boundaries, key standard practices, working vocabulary, and potential hand-off opportunities
- **Physical Exercise**: Participants from each collaborative area looked for hands-on skill improvement in key areas such as protocol analysis, infrastructure awareness and analysis, technology and configuration control, and live incident response. Cross-training of skills and supported introduction of technologies both played significant roles in challenge events.
- **Tabletop Scenario Walk-through**: Key personnel from each sector led a live walk through of a wide variety of scenarios that involved inter-agency hand-off, joint activities, authority boundary maintenance, and resolution of hierarchy of authority. In addition discussions of escalation options, procedures for accessing resources, and review of role interactions took place as prompted by questions from the participants in the audience. The walk-through led to a significant set of questions regarding governmental response to private sector events and how privacy, intellectual property protection, and access assistance/controls would be handled during events.
- **Technology Reviews**: Private and governmental partners both brought tools to the collaboration by presenting them in review sessions. The tools covered a broad range of areas including the commonly used tools in the commercial world where joint activities are likely to occur. This set ranges from protocol analyzers and event log aggregators to scanners and detection systems.
- **Simulation Challenges:** The Colorado National Guard provided access to a scenario-based participant-vs-machine game that provided challenge events and learning opportunities.
- **Hands-on formal Tool Training**: Various groups provided specialized forensic, investigation, and defense tools that supported joint operational awareness.

The collaborative leadership maintains and supplements this list in preparation for each major event as needed. Various participants then formulate contents between events. Regis faculty advocated for maximizing re-use and efficiency by structuring modularity at each scale of deployment. This modularity facilitated constructing the event, designing each event component, and tuning the component performance on the fly based on immediate feedback or facilitator awareness of participant issues.

## 6 Analysis of Outcomes

Generally, the National Guard provided a clear after-action report for the collaborative events. Results of this report proved useful in triggering event improvements as quickly as the very next event. The first major finding was that National Guard team members were organizing their leadership structures internally on an *ad hoc* basis rather than having it imposed by collaborative leadership or pre-existing rank. The room observers noted that leadership and organization of National Guard teams participating in exercises was not formed with common expectations and in the future this would need to be addressed. The standard organization hierarchy that exists

outside the scenarios does not appear to apply in a small-group incident response team as much as experience in technical response and knowledge on incident response procedures.

Second, the team learned that providing a clear process and procedure for self -evaluation and skill assessment yielded significant value. Initially, without clear direction participation in assessments was erratic. The data from those evaluations were used internally by each collaborative entity for identifying training needs of the groups and as a basis for improving the event modules. While the collaborative leadership team did not track participant technical progress individually, they considered that moving to a personalized tracking model might be good. At this time the collaborative leadership team is reviewing logistical and inter-agency policy issues that might present challenges in this area. The specific point in the agenda when post-tests were administered turned out to be significant. The collaborative leadership discovered in the first collaborative event that testing too close to the event end resulted in less participation and loss of attentiveness to detail.

The AGILE method employed by Regis to achieve successful events was not deployed inside the participants' teams during physical exercises. There was a significant delay in some groups particularly when physical exercises began. After discussion with the teams, the gap here may have been because the Regis facilitators were accustomed to working with greater ambiguity of objectives and rapidly self-forming into working groups, so some details had not been sufficiently addressed or described as the scenario was delivered. This suggests that in the future, the team building scenarios will need to design clearer expectations and more detailed structure to more fairly simulate an operational situation.

Developing common vocabulary regarding tools, policy, and logistics turned out to be a big factor linked to the expression of situational needs. Without clear understanding of the full vocabulary involved in a multi-agency situation, miscommunication occurred through assumption or alternative interpretation. With a common vocabulary, efficiency appeared to increase among those groups.

The Colorado Guard had specific desires to cover specific technologies like real-time packet capture analysis, socialize the different groups, ensure all parties understand each sector's leadership hierarchy and roles, and build response team skills and relationships. This went a long way in making the gap analysis effective prior to the collaborative events. Regis' initial requirements were more ambiguous in terms of general improvement of processes, capability, and team knowledge. The challenge for the Regis facilitators was ensuring that the events ran smoothly on a technical and logistical level. The State of Colorado also came with more general goals of collaboration and training, but their early representation in the formative meetings meant that both individual agency and multi-agency collaboration goals would be possible.

## 7 Conclusion

The Guard, the State of Colorado, and Regis have reaffirmed a strong commitment to continue with the Cyber Security Multi-agency Collaboration for Rapid Response

exercises. The collaborative extended the joint effort to more readily include the private sector. Within less than a month after the initial grant review the collaborative leaders established a public-private round table panel linking the public and private sectors. This round table both disseminated results of the grant activities and collected needs from the private sector in order to reset the next round of event goals. The next planned event extends the working relationship and expands the depth and breath of content areas resulting in an advancement of technical, communication and interpersonal skill and knowledge. The collaborative leaders' analysis of the first year's cycle also resulted in refinement of the Xmodel.

The leadership and the technical teams providing training resources continues to successfully use AGILE approaches as part of ongoing collaborative events. The largest adaptation of the AGILE model during the grant period was not in provisioning technical resources for the project, but in controlling a "protocol bleeding" of operational expectations of AGILE methodologies unchecked into assumptions about scenarios. It became clear that because of the need to focus on policy and protocol integration, many functions that the collaborative addressed could not be fulfilled with either AGILE modeling or the Framing Forward Model.

**Bibliography**


1. White, Gregory B., and Dwayne Williams. The Collegiate Cyber Defense Competition. In: Proceedings of the 9th Colloquium for Information Systems Security Education (2005)
2. Novak, H, Likarish D, Moore E. Developing Cyber Competition Infrastructure Using the SCRUM Framework. In: Dodge, Ronal C. Jr., Fuchts, Lynn (eds.) Information Assurance and Security Education and Training. Springer Berlin Heidelberg, 20-31 (2013)
3. Cooper, S, Nickell, C, Piotrowski, V, Oldfield, B, Abdallah, A, Bishop, M, Caelli, B, Dark, M Hawthorne, E, Hoffman, L, Perez, L, Pfleeger, C, Raines, R, Schou, C, Brynielsson, J, An Exploration of the Current State of Information Assurance Education. In: Impagliazzo, John (ed.) Inroads - SIGCSE Bulletin Volume 41, Number 4, December 109-125 (2009)
4. United States Air Force Fact Sheet, http://www.afspc.af.mil/library/factsheets/factsheet_print.asp?fsID=3649
5. Verison, 2014 Data Breach Investigations Report (2014) found at http://www.verizonenterprise.com/DBIR/2014/
6. Hoffman, L., Rosenberg, T., Dodge, R., & Ragsdale, D. . Exploring a National Cybersecurity Exercise for Universities. In: Donner, Marc (ed.) *Security & Privacy,* IEEE, 3(5), 27-33 (2005)
7. Smith NC. The case study: a useful research method for information management. Journal of Information Technology (Routledge, Ltd.). 5, 3, 123. ISSN: 02683962 (Sept. 1990)
8. Manifesto for Agile Software Development, http://agilemanifesto.org/ (2001)