Enhancing Cyber Defense Preparation Through Interdisciplinary Collaboration, Training, and Incident Response

Tristen K. Amador
Regis University
Denver, CO, USA
tamador@regis.edu

Roberta A. Mancuso
Regis University
Denver, CO, USA
rmancuso@regis.edu

Erik L. Moore
Regis University
Denver, CO, USA
emoore@regis.edu

Steven P. Fulton
United States Air Force Academy
USAFA, CO, USA
steven.fulton@usafa.edu

Daniel M. Likarish
Regis University
Denver, CO, USA
dlikaris@regis.edu

***Abstract*—To enhance the capabilities of a cyber defense collaborative, a psychometric analysis team was embedded in a collaborative incident response team. Collaborative incident response community members included the State of Colorado, the Colorado National Guard, Regis University, private companies, and others. The collaborative training developed when National Guard leadership saw the Rocky Mountain Collegiate Cyber Defense Competition held at Regis, and planning began around the potential of collaborative training. The case presented shows the progressive efforts that allowed this to move from enhancing training exercises to being embedded during live cyber defense operations. Some outcomes of the psychometric evaluation are presented here as an embedded quantitative study within the framing case analysis. The case analysis is then used to formulate a generalized model designed to support opportunities for a range of interdisciplinary collaboration in support of technical endeavors with operations security requirements as exemplified by cyber defense. The resulting model provides a framework for expanding research to other disciplines.**

Keywords—Interdisciplinary Collaboration, Psychometrics, Psychometric Analysis, Sociotechnical, Cyber Defense, Cybersecurity, Collaborative, Incident Response, Colorado National Guard, Cybersecurity Training, Incident Response, Trust, Myers-Briggs Type Indicator, MBTI, Parker Team Player Survey, PTPS, Crew Cohesion Assessment Tool

I. Introduction

To develop a roadmap for enhancing cyber incident response, an inter- organizational coalition of state governments, military defense teams, industry, and academic partners in the State of Colorado deployed psychometric analysis during a series of training exercises to address the sociotechnical dynamics in cyber defense activities. This paper details the pathway that enabled this interdisciplinary collaboration. It also presents a generalized model that may be used as a template for technical teams with operational security requirements that are attempting to extend beyond technical protections by leveraging relevant interdisciplinary expertise. A collaborative training and response community (CTRC) evolved from a group of like-minded academic, state, military, and industrial sector members. The authors' work with this group incrementally advances a trusted training environment where multiple interdisciplinary experts can be embedded with a defensive team to extend traditional incident response methods. Once trust and relationships were established in the training environment, the new capabilities could be used in live incident response.

The specific case presented in this paper incorporates psychometric analysis and feedback to enhance the adaptability of personality types and, ultimately, improve overall team performance. Initial observations took place during a Rocky Mountain Collegiate Cyber Defense Competition (RMCCDC) where the CTRC was also observing. It was during the competition, which involved the defense of a simulated financial institution, that the concepts regarding the teamwork analysis were formed and shared among the CTRC. Next, the psychometric analysts on the Regis faculty engaged the collaborative community in discussions regarding possible inclusion of psychometric analysis as another way of strengthening the cyber defense teams to be even more effective. In May of 2017, the analysts administered a series of tests to assess personality types and team player styles to better understand how successful teams work together.

II. Case Background

Since the RMCCDC is a large event held on a satellite campus of Regis, several faculty members from other disciplines at this satellite campus were aware of the cyber competition and suggested using a psychometric team analysis process to study the ongoing cyber team response. The close co- location of faculty members from different disciplines at this campus was critical in the early interdisciplinary brainstorming sessions and ongoing discussions.

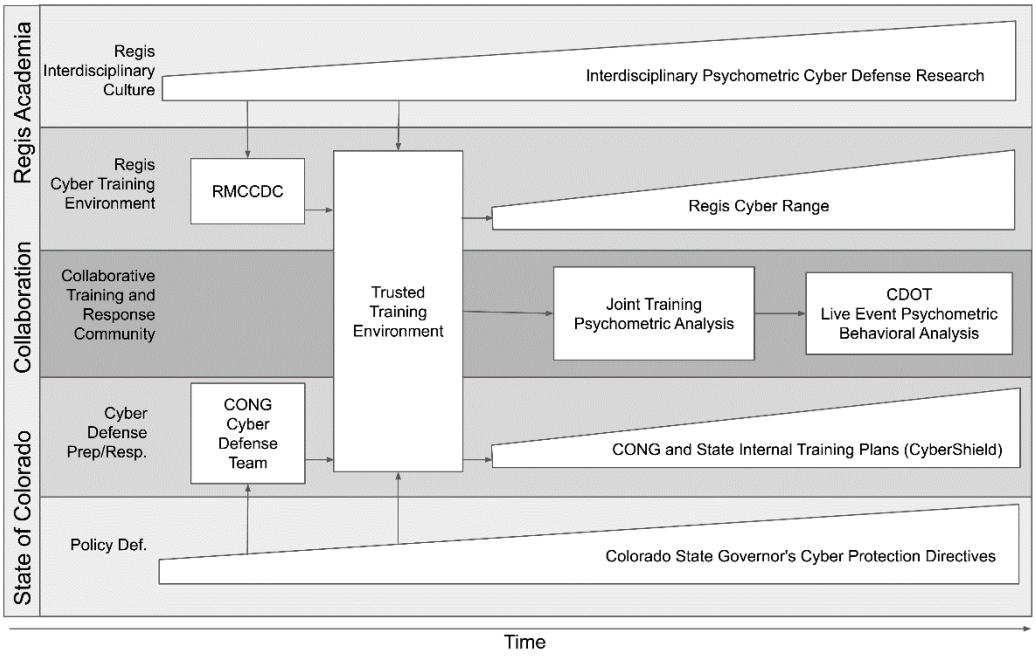

Fig. 1. Environment portraying the integration of psychometric analysis as part of an interdisciplinary effort. This analysis became a resource of the established trusted training environment.

This interdisciplinary organization of academics along with the CTRC, comprised of Colorado State employees, Colorado National Guard (CONG) military personnel and cyber industry experts began to jointly create a trusted training environment in which mistakes could be made without attribution and skills could be developed. This specific environment is outlined in Figure 1. The cross dimensional work identified as the Trusted Training Environment became the central pillar of the CTRC. It was here in this trusted environment where the differing organizations learned to trust each other. It was this environment that is the basis of our psychometric analysis training work. Details of this experience can be found in our earlier work [1]. As time went by, the level of trust following these events increased between each of the organizations. This allowed the research team to suggest new ways for the teams to work and new team environments in which to work.

There were two principle influences leading to the implementation of the Trusted Training Environment. The first was the progressive and incremental implementation of an early, competition-based challenge beginning with the CANVAS (Computer and Network Virtualization and Simulation) joint student technical and business training exercises supported by Regis University (RU) and the United States Air Force (USAF) [2]. The second was the decision to offer the RMCCDC [3] in Denver. The RMCCDC is a two-day collegiate cyber security team competition, established in 2005 [4]. RMCCDC offered physical cyber security exercises requiring the implementation of significant server and network infrastructure. This infrastructure allowed the RU cybersecurity faculty to offer collaborative training opportunities to local and state government agencies, the Colorado National Guard, private industry and critical infrastructure organizations, forming a CTRC. In the early days of our exercises, this community focused on advancing technical skills, providing RU the opportunity to build out a complex cyber range. When the community reached targeted levels of technical proficiency, the CTRC leaders observed that team performance could be further enhanced with non-technical training. This led to initial psychometric observations that were made during a recorded training exercise and was confirmed during the After Action Report (AAR) by the CTRC psychometric analysts. After these observations, the CTRC expanded activities to include the interdisciplinary psychometric analysts and formed the research team. Efforts to pilot the inclusion of psychometric analysis by RU in collaboration with the exercise partners resulted in incorporating team building that could enhance team performance. Based on those early interdisciplinary interactions, professors in health care management and psychology led to the addition of psychometric analysis to the capabilities employed to enhance cyber defense team performance. The case below came out of these initial interactions.

III. Case Methodology

An embedded case study methodology is an appropriate research instrument for analyzing the insertion of psychometric research into a collaborative environment requiring high levels of trust. Creswell and Creswell's embedded case study methodology [5] is based on a post-positivist perspective and is designed to address

sociotechnical dynamics. The authors used as the example a cross-sectional study, where the application of the Myers-Briggs Type Indicator (MBTI) and the Parker Team Player Survey (PTPS) instruments provided analytic tools in an effort to enhance performance within cybersecurity training environments that require operations security. The case includes brief qualitative analysis to provide a reference for a generalizable model of integrating experts from diverse disciplines within cyber defense training, and provides a reference case for facilitating this type of work. Embedding a quantitative research methodology into a case study has been explored previously as Scholz and Tietje described in 2002 [6] and guided us in creating a model for injecting a range of disciplines into technical training environments requiring high levels of trust because of factors like operational security requirements.

The questions this work answers are the following: Is there a viable path to incorporate interdisciplinary expertise and tools into a cyber defense training program and incident response operation? Also, is there a generalizable model that can be abstracted from the case that might be transferable to other cyber defense situations and other interdisciplinary work? Prior to the research questions described here, the leadership of the CTRC started by asking how we could work together to "make a good team even better." This initial question drove the authors to formulate the research questions as we looked outside the cyber defense discipline for methods of enhancing operational capabilities. Working with psychometric analytical techniques and embedding this in a larger framework is the method we chose to provide a formal method of reflection on the efficacy of this work. The insights in the conclusion are formulated into a generalizable model designed to guide future work.

IV. Case Research Context

High functioning teams in cyber security incident response are critical given the prevalence, substantial cost, and rising complexity of cybercrime. In regard to medical and other types of incidents, Uitdewilligen *et al*. describe "multidisciplinary crisis management teams consist of highly experienced professionals who combine their discipline-specific expertise in order to respond to critical situations characterized by high levels of uncertainty, complexity, and dynamism" [7]. Cybersecurity teams are characteristic of these highly experienced professionals working within uncertainty, complexity, and dynamism that Uitdewilligen *et al*. discuss. Our research suggests that convening and responding as a collaborative and cohesive team are vital to a team's success, yet we have much to learn about how we intentionally create these high-functioning, collaborative teams.

Willems *et al*. [8], in discussing disaster response in the medical field, describe some of the interprofessional, non-technical skills needed which include skills such as "physical self-care including survival skills, psychological self-care, flexibility, adaptability, innovation, and improvisation" which they call the "skills for austere environments." Additional skills identified by Willems *et al*. include cognitive strategies such as "big picture thinking, situational awareness, critical thinking, problem solving, and creativity". Interprofessional attributes include characteristics such as "communication, team-player, sense of humor, cultural competency and conflict resolution skills". Other studies support the importance of non-technical skills in incident response teams. For example, Tokakis *et al*. [9] found that leaders with strong decision-making abilities, communication skills, and emotional intelligence were instrumental in the integration of crisis management teams in the public sector.

Another study investigating non-technical skills included software engineers and concluded that specific attributes such as managing expectations, creating a "safe haven," asking for help, creating shared success, and perseverance are key attributes among the most expert of engineers [10]. Li *et al*. state, "this reinforces the perspective that software engineering is a sociotechnical undertaking, and not just a technical one." Additionally, much of the work of Li *et al*. also focused on the importance of effective decision making among software engineers, especially as they are "tasked with making decisions in increasingly more complex and ambiguous situations, often with significant ramifications."

Numerous studies suggest that additional skills, beyond technical skills, impact team effectiveness in incident response. What remains unclear is how to develop and ultimately advance team-work skills in more insular technical cultures, specifically in a cybersecurity team. Our research suggests that one way to further develop the human side of cyber skills is to more fully understand personality trait preferences and role diversity of cyber team members. Utilization of instruments such as the MBTI may be important for team development because past studies [11] have indicated that the MBTI can successfully predict group performance in crisis management; it also successfully predicts the style in which individuals communicate, make decisions, and manage change and conflict.

Further, because certain personality types tend to be over-represented in certain careers [12], it may be advantageous to develop strategies that capitalize on or compensate for the ways that particular personality types prefer to contribute in their social and work environments. As cited in Hammer [13], people who prefer Introversion on the MBTI are more likely to choose careers that do not necessitate frequent social interaction, such as Information Technology (IT). In addition, people who prefer the Sensing and Thinking (ST) facets of the MBTI tend to be drawn to facts and objective analysis [14]. They often choose careers that are technical and practical in nature, consistent with positions in IT as well as law enforcement and the military [15]. In studies of organizational team performance, ST individuals also tend to show the most risk avoidance and are more inclined to take risks only in an environment consistent with their type [16]. In addition, the researchers measured Crew Cohesion, a global assessment of team performance.

Both role and type diversity within teams are variables that predict team performance. Research on team-work

suggests that diverse groups often perform better, working more quickly and more consistently than similar groups [17]. The Parker Team Player Survey (PTPS) is an assessment tool that identifies role diversity, specifically whether team members perform primarily as the communicator, collaborator, challenger, or contributor [18]. Teams that encompass all of these roles are theorized to be most effective. Utilizing established assessment tools is critical as we begin to understand how cyber defense teams can work together to ensure rapid, efficient, and effective response to the ever-changing landscape of cyber threats.

V. Background of the Psychometric Analysis

Our exploratory research included a pilot study that focused on personality trait preferences and role diversity within the CONG. The CONG team is comprised of cyber defense experts. The members of this team had been working together in CTRC exercises for several years and use a leadership structure based initially on individual military rank and civilian government leadership, adjusting this with individual skill set. Inclusion of an active cyber defense team is a unique feature of our research.

The cyber defense physical exercise analyzed in this pilot study used the scenario of defending a financial institution. As described earlier, this was developed originally as a challenge for the RMCCDC to allow the visiting college teams to identify and recognize vulnerabilities in a networked environment. The exercise was repurposed for the CONG exercise for two reasons: to allow the cyber defense teams to practice their expert technical skills and team collaboration, and to allow the researchers to observe type and role diversity within the CONG during a challenging training exercise.

VI. Psychometric Methodology and Results

In the pilot, the authors hypothesized that team members would show greater preference for Introversion versus Extroversion, Sensing versus Intuition, and Thinking versus Feeling on the MBTI, in contrast to preferences reported by the general population. An additional hypothesis was that teams with greater role diversity (exhibited by the PTPS) would exhibit better performance. The Crew Cohesion Index will be used to track the team's effectiveness over time.

Thirteen members of the CONG (11 men, 2 women) participated in a cybersecurity exercise at Regis University. Of the participants, eleven were Caucasian, one was African American, and one was Asian. The median age of participants was 35, with ages ranging from 28 to 47 years. Approximately 46% had college degrees. Of the 13 participants, 54% had worked together as a team. Approximately 42% considered themselves to be novices in cybersecurity, while 58% had at least some level of experience.

Myers-Briggs Type Indicator. The MBTI personality inventory was used to identify the variability of personality type in each team. It is a highly valid and reliable research-based assessment tool that has been in use for over 60 years. According to the Myers Briggs Company, over 88% of Fortune 500 companies use the MBTI as a hiring tool and hundreds of universities use it as an assessment tool. Approximately 1.5 million individuals complete the MBTI online each year [19]. MBTI certified practitioners engage in a minimum of 30 hours of training in order to administer the MBTI and interpret the assessment results. Moreover, there are several thousand peer reviewed research studies that have utilized the MBTI. Researchers and practitioners who are experts in survey methodology and personality assessment confirm that it is one of the most scientifically sound measures of personality type in the field of psychology.

The MBTI identifies differences in personality type using four central dichotomies, two that capture differences in attitudes (Extraversion – Introversion and Judging – Perceiving) and two that capture mental functions (Sensing – Intuition and Thinking – Feeling) [14].

The Parker Team Player Survey [18] is a reliable and valid assessment tool that identifies the level of role diversity within a team environment. In team activities, each member brings with them a specific set of strengths based on a combination of personality, communication and leadership skills, and past experience. The PTPS assesses the current strengths of each individual and suggests ways to increase each person's effectiveness as a team player. In the current study, participants were asked to indicate the role they typically perform (communicator, contributor, collaborator, or challenger) in team settings.

The Crew Cohesion Assessment Tool [20] assessed team performance during the cybersecurity exercise, including the quality and quantity of collaboration, communication, team rapport, and team cohesiveness.

Of the seven participants who completed MBTI assessments, three reported Extraversion as their type preference while four reported Introversion. Six of our participants preferred Sensing while one participant showed a greater preference for Intuition. Finally, all seven participants showed a greater preference for Thinking rather than Feeling. All 13 participants completed the PTPS to assess their role diversity. Results indicated that four were Contributors, three were Collaborators, two were Communicators, and none were Challengers, with the remaining participants exhibiting dual roles that did not include the Challenger.

Trends in the data gathered from the Crew Cohesion Assessment showed slight decreases in Communication, Trust, Effectiveness, Leadership, Teamwork, and Conflict as the exercise progressed.

Preliminary findings of the pilot support our hypothesis that there would be a greater preference for Introversion rather than Extraversion. Also consistent with the hypotheses, we found a greater preference for Sensing versus Intuition, with only one participant preferring Intuition. This is in contrast to the general population, where 70% prefer Sensing and 30% show a preference for Intuition [14].

Also supporting the hypotheses, there was an oversampling of Thinking versus Feeling. This is consistent with qualities predominant in the fields of IT, law enforcement, and the military, and is in contrast to the general population, where 60% indicate a preference for Thinking versus 40% for Feeling [14]. PTPS data showed moderate role diversity, with three of the four roles represented.

These findings suggest for those intentionally constructing and developing cyber teams that strategies leveraging type and role diversity may improve performance. For example, cybersecurity response teams could benefit from the ability to attend to both details and the bigger picture. Thus, diverse team members with Sensing and Intuition, could approach their task with greater flexibility and creativity when generating solutions to cyber threats. A team that incorporates both logic and emotions (i.e. both Thinking and Feeling) could exhibit greater cohesion, exhibited by increased trust, enhanced teamwork, and more effective conflict management [8]. Moreover, increasing diversity along both the Sensing-Intuition and Thinking-Feeling dimensions could encourage less risk avoidance, a critical piece of crisis management [16]. Drawing from research on the PTPS, it could also benefit response teams to include a team member who can adopt the role of Challenger to present difficult questions and question accepted paradigms [18].

Similar to preliminary results in the pilot, research from Willems *et al*. [8] on the non-technical skills of disaster response teams in the medical field also suggests that diversifying team type enhances performance. For example, Willems *et al*. stress the importance of flexibility, adaptability, improvisation, big picture thinking, and creativity as critical non-technical skills for team members. Willems *et al*. suggest that inter-professional attributes such as communication, team-player, and conflict resolution skills could significantly diversify the knowledge, skills, and effectiveness of team members. Willems *et al*. also suggests that "effective teamwork, clear leadership, role adjustment, and conflict resolution" are skills that disaster response teams should focus their development efforts.

Tokakis *et al*. [9] recommend that leaders of crisis management teams specifically improve their emotional intelligence competencies in order to enhance overall team integration and performance as well as goal attainment. Noting that the Crew Cohesion scores were decreasing as the pilot exercise progressed, observation also suggests that further training emphasis on leadership core competencies and emotional intelligence could address this.

While the pilot study had the inherent limitation of small sample size, the observations in the pilot and the work of Tokakis *et al*. [9] suggest that further work developing and testing psychometric instruments could support the goal of identifying qualities that embody more effective cyber response team members. Such work in the future should incorporate larger numbers of participants since small sample size was a limitation in this study.

VII. Generalizing the Psychometric Case

In order to assist those with similar goals of increasing collaboration with teams requiring operational security, the authors generalize the interdisciplinary environment in Figure 2, modelling the embedded psychometric analysis of cyber defense training into embedded interdisciplinary support for a trusted training environment.

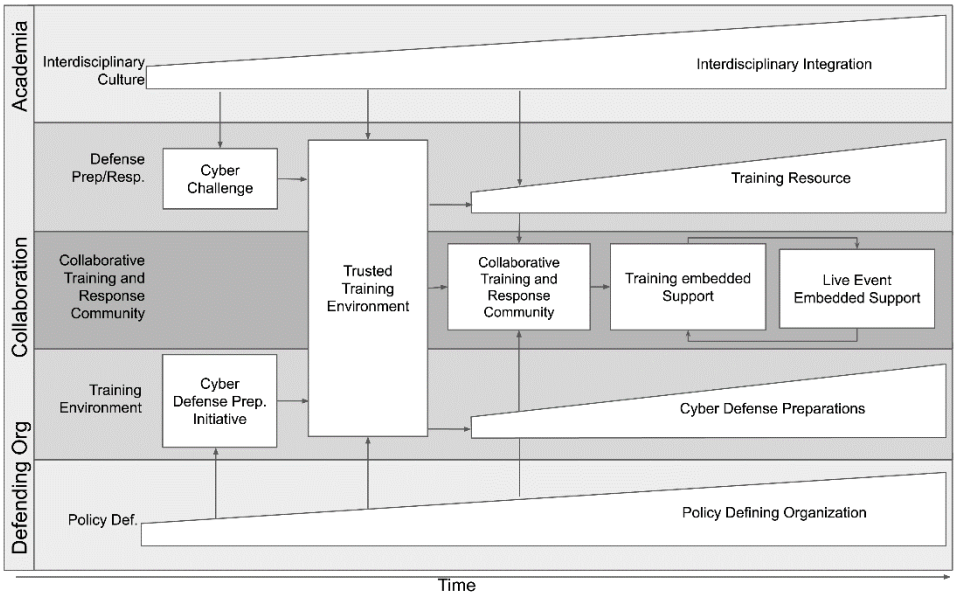

Fig. 2. Generalized model portraying the integration of embedded support as part of an interdisciplinary effort. This new embedded support becomes a resource of the established trusted training environment.

The model identifies a roadmap connecting academia and a defending organization resulting in a CTRC. This is achieved by identifying bridge points connecting their internal development paths to achieve a common trusted training environment. These bridge points, represented by arrows in Figure 1, include interdisciplinary observations, training pilots, and policy adjustments that demonstrate incremental value. Applying this model to the analysis of additional cases could result in enhancing training and live incident response for a variety of incident response teams that may not yet have the advantage of interdisciplinary support. The model from top to bottom is formulated to reflect the bridging of complex academic organizational cultures and their interaction with quite disparate groups like military units, civilian government agencies, other academic institutions, and private security companies.

The authors intend to apply the generalized model across a broader range of cyber incident responders, digital business continuity teams, and disaster recovery policy development. In addition, the team is identifying places to use interdisciplinary contributions to technical degree programs. This harkens back to the original discussion between the cyber defense community and the psychologists, suggesting that they were looking for ways to "make strong teams even stronger."

REFERENCES

[1] Moore, E., Fulton, S., Mancuso, R., Amador, T., Likarish, D., (2019, June), A Short-cycle Framework Approach to Integrating Psychometric Feedback and Data Analytics to Rapid Cyber Defense. Information Security Education, Education in Proactive Information Security, IFP AICT 557, proceedings of the 12th IFIP WG 11.8 World Conference, WISE 12

[2] Collins, M., Schweitzer, D., & Massey, D. (2008, June). Canvas: a regional assessment exercise for teaching security concepts. In Proceedings from the 12th Colloquium for Information Systems Security Education.

[3] Regis University Site for the Rocky Mountain Collegiate Cyber Defense Competition, https://rmccdc.regis.edu/rmccdc/

[4] White, G. B., & Williams, D. (2005, October). The collegiate cyber defense competition. In Proceedings of the 9th Colloquium for Information Systems Security Education.

[5] Creswell, J. W., & Creswell, J. D. (2017). Research design: Qualitative, quantitative, and mixed methods approaches. Sage publications.

[6] Scholz, R. W. & Tietje, O. (2002). Embedded Case Study Methods: Integrating Quantitative and Qualitative Knowledge. London: Sage Publications Inc. ISBN 0-7619-1946-5

[7] Uitdewilligen, S., and Waller, M. J. 2018. "Information Sharing and Decision- Making in Multidisciplinary Crisis Management Teams," Wiley Journal of Organizational Behavior (39), pp. 731-748.

[8] Willems, A., Waxman, B., Bacon, A. K., Smith, J., Peller, J., and Kitto, S. 2013. "Interprofessional Non-Technical Skills for Surgeons in Disaster Response: A Qualitative Study of the Australian Perspective," Journal of Interprofessional Care (27), pp. 177-183.

[9] Tokakis, V., Polychorniou, P., and Boustras, G. 2018. "Managing Conflict in the Public Sector During Crises: The Impact on Crisis Management Team Effectiveness," International Journal of Emergency Management (14:2), pp. 152- 166.

[10] Li, P.L., Ko, A.J., and Zhu, J. 2015. "What Makes a Great Software Engineer?," in Proceedings of the 2015 IEEE/ACM 37th IEEE International Conference on Software Engineering, Florence, IT, pp. 700-710.

[11] Sample, J. A., and Hoffman, J. L. 1986. "The MBTI as a Management and Organizational Development Tool," Journal of Psychological Type (11), pp. 47- 50.

[12] Schaubhut, N. A., and Thompson, R. C. 2008. MBTI Type Tables for Occupations, Mountain View, CA: CPP, Inc.

[13] Hammer, A. L. 1993. Introduction to Type and Careers, Mountain View, CA: CPP, Inc.

[14] Myers, I. B., McCaulley, M. H., Quenck, N. L., and Hammer, A. L. 2009. MBTI Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator Instrument, Mountain View, CA: CPP, Inc.

[15] Beyler, J., and Schmeck, R. R. 1992. "Assessment of Individual Differences in Preferences for Holistic-Analytic Strategies: Evaluation of Some Commonly Available Instruments," Educational and Psychological Measurement (52:3), pp. 709-719.

[16] Walck, C. L. 1996. "Management and Leadership," in MBTI Applications: A Decade of Research on the Myers-Briggs Type Indicator, A. L. Hammer (ed.), Mountain View, CA: CPP, Inc., pp. 55-80.

[17] Blaylock, B. K. 1983. "Teamwork in a Simulated Production Environment," Research in Psychological Type (6), pp. 58-67.

[18] Parker, G.M. 2008. Team Players and Teamwork (2nd ed.), San Francisco, CA: Jossey-Bass.

[19] The Myers-Briggs Company. 2017. The Myers-Briggs Type Indicator (MBTI). Retrieved June 30, 2020 from https://www.themyersbriggs.com/en-US/Products- and-Services/Myers-Briggs.

[20] WFLDP Toolbox. 2018. Crew Cohesion Assessment Tool, April 16. (www.fireleadership.gov, accessed October 20, 2018)