Design and Evaluation of a Cyber Protection Team Planner Work Aid

Kristen Liggett, Arielle Stephenson, Meghan Strang and Geoffrey Dobson
Air Force Research Laboratory, WPAFB, OH USA
Kristen.Liggett@us.af.mil
Arielle.Stephenson.ctr@us.af.mil
Meghan.Strang.1@us.af.mil
Geoffrey.dobson.1@us.af.mil

Abstract: Cyber Protection Teams (CPTs) are responsible for providing mission assurance by ensuring that mission-relevant cyber terrain is secure and protected for operations. In order to do this effectively, CPT planners must correlate and integrate information regarding customers’ missions with information about the systems and networks required to perform those missions. To support this challenge, a CPT Planner work aid was designed and evaluated to assess its effectiveness. The evaluation compared the work aid with current CPT planning methods. Ten participants with varying planning expertise performed four planning tasks (managing approvals, assigning resources, managing accesses, and scheduling meetings). To test the efficacy of the proposed work aid, participants were tasked with planning a fictional mission utilizing both the traditional planning method and the work aid method. Data was collected from objective metrics to include time and task performance score, as well as subjective perception of workload. In addition, participants were asked a series of situation awareness (SA) questions after each task to measure their understanding of the mission-relevant information. Score and time to answer SA questions were also recorded. While CPT planning experience did not have a significant effect on performance, results revealed significant improvements in task time, SA question response time, and perceived workload when using the work aid versus the baseline condition.

Keywords: cyber protection teams, work aid design, situation awareness metrics

1. Background

The cyber domain is one of incessant progress and growing emphasis in warfare operations. Within this dynamic field, cyber security and cyberspace operations sit in a state of unrest. Cyberspace is defined by Air Force Doctrine Annex 3-12 Cyberspace Operations as a “global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers” (United States, 2011). Cyberspace operations consist of military activities to identify, degrade and/or deceive threat actors in a virtual space, while cyber security functions to ensure network operations are trustworthy (Trent et al., 2016). As technology and computers continue to play a prominent role in everyday activities across the world, the Department of Defense (DoD) has recognized the potential threats that accompany this surge in cyber usage. In order to defend and protect against these inherent risks, U.S. Cyber Command was established in 2009 and further expanded into multiple task groups including Cyber Mission Teams and a Cyber National Mission Force in 2012 (Lathrop, Trent, and Hoffman, 2016; U.S. Army Cyber Command, 2020).

The DoD’s establishment of cyber-specific tasks groups has been a critical advancement in the endeavour to maintain cyberspace dominance. However, these unique groups have emerging capabilities and therefore new requirements that must be assessed. For example, operators in the field require certain skillsets and tools in order to properly assess situations and determine appropriate courses of action. Operators have reported that even when tools are accessible, they are often non-functional, are not fully understood by the operator(s), or are becoming outdated (Anderson, 2018). Additional unique limitations arise from the design space for these tools. For example, cyberspace tools are often built by and for networking experts who have full privileges and access within the network while they are designing the tool, and these conditions rarely exit for teams in an operational setting (Trent et al., 2016). Additionally, a qualified operator may have accessibility to the necessary tools, but obtaining the required permissions to utilize them cause a major setback in operations. As stated in Cyber Network Mission Dependencies, “Because all DoD missions depend on cyber infrastructure, failure to secure network assets and assure the capabilities they enable will pose a fundamental risk to any defense mission,” (Schulz, Kotsin, and Gibson, 2015). With rapidly evolving technological advancements across the globe, it is critical that operators are equipped with useful and usable tools in order to remain vigilant.

The Cyber Mission Force is constructed of various types of teams, each with respective assignments that contribute to the overall mission. Among the support teams are Cyber Protection Teams (CPT), which serve to defend information networks, prepare operational cyber forces, and protect high priority missions (U.S.
Congressional Research Service, 2020). CPTs must provide expert skills and core competencies in order to mitigate threats and assure mission readiness. The four main mission types conducted by CPTs include network assessments, incident response, threat assessment, and active defense (Lathrop, Trent, and Hoffman, 2016). As of 2019, CPTs lack a planning tool and instead rely on a shared information repository (Pomerleau, 2019). This contains a combination of spreadsheets, typed documents, and hand-written visuals which provide the necessary information for planning missions. While this type of information allows the user access to available resources, the fact that they are all in different formats (some are hard copy only) and the information is not integrated results in increased planning time and cognitive load. Therefore, the objective of this study was to design and evaluate a CPT planning tool in order to increase the efficiency and effectiveness in which planners can execute their tasks.

2. Design process

The CPT Planner work aid was designed using the Human Factors Design Process. This process consists of an analysis phase and an iterative design phase. This section will describe these phases along with a description of the work domain analysis results.

2.1 Analysis phase

During the analysis phase, the work domain was analyzed by conducting literature reviews, participating in relevant workshops, attending demonstrations of relevant software, conducting targeted topic area discussions, participating in cyber exercises, and visiting various operational sites. Knowledge acquisition (KA) activities were conducted with a number of CPT planners and subject matter experts (SMEs) in the area of mission planning. Additionally, research was conducted at United States Transportation Command (USTRANSCOM) and firsthand observations were made of CPTs being tasked and responding to a mission. The design team also received artifacts from CPT planners that gave insight into the types and format of information required to perform their tasks, as well as how they administered or completed said tasks using current methodologies and practices.

2.2 CPT planner workflow

CPT planning is initiated with the receipt of a task order to support a particular mission. The CPT planner reviews the information provided on the task order and then determines what additional information is needed. This information must be requested from mission owners, network owners, and system owners, and is currently done via email to the various points of contact (POCs). Typically, POCs are identified in the task order, however, if they are not, the CPT planner must track them down. While waiting for information requests to be filled, the CPT planner reviews CPT actions that are pre-approved for the mission and listed on the task order. The planner determines if additional approvals for action on the mission relevant cyber terrain are required and will request additional approvals if necessary. The CPT planner cannot begin their mission until the appropriate approvals have been received from the POC. Following approvals, the planner must determine further resources that are required to conduct the mission. This includes determining which members are qualified to utilize the tools needed to perform necessary tasks, along with analyzing those members’ availability. If certain tasks require various network or building access, these must also be requested based on task assignments. The final planning step includes scheduling a variety of meetings with the mission owner.

Based on the aforementioned task flow, it was determined that CPT planning activities center around four major tasks: identifying and requesting approvals to perform certain actions on networks/systems of interest, allocating trained operators to perform required tasks, obtaining access to various systems and networks identified as mission relevant cyber terrain, and communicating the mission plan via multiple meetings with various people (the team, mission owner, network points of contact, etc.). These tasks are critical to planning operations yet they are currently conducted with no specific planning tools. Instead, planners rely on spreadsheets, documents, pdfs, electronic calendars, training records, email, whiteboards, and sticky notes to organize and compile information. In consideration of the unique requirements within each mission, this process easily becomes tedious and timely for planners who often operate in time-constrained environments.

2.3 Iterative design phase

The information gathered during the analysis phase was transformed into a work aid prototype designed to facilitate the accomplishment of the four key CPT tasks. The planning process was streamlined through the integration of relevant information and the use of automation. In the iterative design phase of the human factors design process, multiple sessions were held with CPT planners and SMEs to receive feedback on the usefulness and usability of the work aid prototype.
3. Method of evaluation

In order to evaluate the effectiveness of the CPT planning work aid design, the prototype was evaluated against a baseline condition. The baseline condition consisted of the use of documents and spreadsheets to perform the four planning tasks described in the CPT Planner Workflow section (managing approvals, assigning resources, managing accesses, and scheduling meetings), mirroring the manner in which activities are currently performed. This condition is referred to as the manual condition due to its need for information to be manually integrated throughout task performance. One interest of this study was to observe the effects of the work aid on CPT members with no planning experience to perform the planning tasks efficiently and effectively. Therefore, this study had two independent variables: planning method (manual versus work aid) and planning experience (novice versus experienced). Fictitious missions were created for participants to plan during training and data collection. Dependent measures included time to complete each task, task performance score, and a subjective workload assessment using a Modified Cooper Harper Scale as shown in Figure 1. In addition to these three metrics, situation awareness (SA) probe questions (Endsley, 2000) were developed and asked after each task to determine if participants understood relevant information. An example of a SA question for the manage approvals task asked, “Do all of the actions necessary to complete this mission have prior approval?”. Time and accuracy of responses to all SA probe questions were recorded.

Figure 1: Modified Cooper-Harper Scale for Subjective Workload Assessment

3.1 Hypotheses

It was hypothesized that there would be a significant interaction between planning method and planning experience in that performance under the work aid condition would not be significantly different across various levels of planning experience, while performance in the manual condition would be significantly different with operator experience. In other words, participants with planning experience would perform better in the manual condition than their less experienced counterparts, while the work aid condition would facilitate statistically similar performance for participants of all experience levels. Additionally, it was hypothesized that there would be a positive correlation between task performance and SA question score, indicating that one should understand the relevant information if they performed well at the task.

3.2 Participants

Participants of the study included ten volunteers within the 837th Cyberspace Operations Squadron at Scott Air Force Base. These individuals were members of various CPTs at USTRANSCOM. Four participants reported having prior CPT planning experience while six did not. Participants completed the study on a voluntary basis with no other incentive than the ability to contribute to scientific research. The study was conducted in a secluded and secure area in order to limit distractions and interruptions.
3.3 Procedure
Participants were assigned to the condition order (manual first versus work aid first) in a counterbalanced fashion. Prior to the start of each condition, participants completed a training and practice portion to ensure a basic understanding of what was expected from each task. For consistency, training was accomplished via a pre-recorded video explaining the procedures for accomplishing the mission for each condition and questions were encouraged throughout this phase. For practice, participants performed a shortened version of each of the four tasks to ensure an understanding of what they were to accomplish. Following the completion of training and practice, participants completed all four tasks within the respective condition and this procedure was then repeated with the other condition. Throughout all phases of practice and data collection, participants rated their perceived workload after completing each task. Following the workload rating, SA questions relevant to the particular task were completed.

4. Results
Results showed that there was no significant interaction between the two independent variables of planning method and planning experience for all five dependent measure (task time, task score, workload, SA time, and SA score). Planning experience had no significant main effects for the dependent measures. However, independent sample t-tests showed significant differences for planning method, results shown in Table 1. Task time, workload, and SA time revealed significantly smaller values for the work aid condition when compared to the manual condition (p < 0.0001), while SA score was significantly higher for the manual condition (p = 0.0077). While the work aid condition yielded higher task performance scores when compared to the manual condition, these results proved insignificant (p = 0.1511).

Table 1: Independent sample t-test results for planning method

<table>
<thead>
<tr>
<th></th>
<th>Work aid (M, SD)</th>
<th>Manual (M, SD)</th>
<th>Test Statistic</th>
<th>P-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task time (Secs)</td>
<td>314.6, 103.8184</td>
<td>1020.3, 179.3743</td>
<td>-11.5033</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>Task score</td>
<td>33.5, 0.9718</td>
<td>32.9, 1.3703</td>
<td>1.1927</td>
<td>0.1511</td>
</tr>
<tr>
<td>Workload</td>
<td>4.4, 0.6992</td>
<td>16.3, 3.566</td>
<td>-7.6388</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>SA time (Secs)</td>
<td>508.6, 132.8953</td>
<td>567.6, 116.46</td>
<td>-1.7331</td>
<td>&lt; 0.0001</td>
</tr>
<tr>
<td>SA score</td>
<td>28.5, 1.841</td>
<td>28.6, 0.81</td>
<td>1.5138</td>
<td>0.0077</td>
</tr>
</tbody>
</table>

Correlations were analyzed between all metrics for both conditions. For the manual condition, SA score and SA time had a moderate negative correlation (r = -0.4974), while task time and task score had low positive correlation (r = 0.3929). SA time and task time revealed a moderate positive correlation (r = 0.5079). For the work aid condition, SA score and SA time had a moderate negative correlation (r = -0.5519), while SA score and task score had a moderately positive correlation (r = 0.631). SA time and task time showed a moderate positive relationship (r = 0.6571).

5. Discussion and conclusion
The results of this study revealed that participant performance while utilizing the work aid was consistently better than when using the manual condition. Participants conducted tasks in statistically significant less time with the work aid condition compared to the manual condition, with the average time being more than 11 minutes faster. SA time was also significantly faster for the work aid condition, resulting in nearly a minute of saved time while upholding significantly higher performance scores. The results are indicative of the work aid’s ability to facilitate high performance while also saving time, avoiding the typical speed/accuracy trade-off that is often observed in social science experiments. This study also revealed lower levels of perceived workload for the work aid condition compared to that of the manual. With an average workload rating of 1.1 (compared to the manual condition’s 4.4), it is clear that the integration of information and automated assistance provided through the work aid saved the operators mental strain as they conducted the tasks.

The correlative analyses throughout this study also pose encouraging results. Literature is clear that situation analysis is an important component of effective task performance yet the development of SA metrics is often challenging in research. Under this consideration, the objective measurement of participant SA was a significant goal of this study. The moderate positive correlation between task score and SA question score suggests that participants with a high understanding of relevant information are performing tasks effectively, thus indicating that that the SA questions focused on appropriate information relevant to task performance.
It was hypothesized that this study would reveal a significant interaction between planning experience and planning method. It was expected that participants with planning experience would perform better in the manual condition compared to their non-experienced counterparts due to familiarity of the conditions, while the work aid would result in higher performance for those with and without experience. These expectations were violated as planner experience did not significantly interact with planning method. A plausible explanation for this violation could be due to the use of fictional missions to supplement the study. CPT planners rely on experiential information (what members are best at which tasks, what actions are typically pre-approved, etc.) to conduct their tasks. However, the advantage of this experience could have been mitigated in the research setting which presented fictitious team members, tasks, orders, and missions for purposes of this study.

The operational environment of CPTs is complex and dictates rapid action in order to continuously defend crucial military networks. The criticality of CPT operations has the potential to be damming if not performed effectively and within the given time constraints. At an organizational level, the prescribed work aid has the potential to momentously improve the overall Cyber Mission Force through its facilitation of increased performance and decreased task time. Given the recent emphasis placed on a highly capable cyber force to maintain global security and stability, advancements for CPTs may have great implications on an international scale. At an individual level, the work aid also simplifies the stressful undertakings that must be performed throughout the planning process on a regular basis. Due to its alleviation of perceived mental workload, the work aid can greatly reduce the occupational stress placed on operators, leading to higher levels of job satisfaction and increased productivity.

In conclusion, planning is a crucial first step in mission execution for CPTs that necessitates tools capable of integrating information from a variety of sources. Automation is needed to minimize unnecessary work and promote timely, effective action that leads to mission success. The work aid proposed throughout this study proved effective at providing these requirements and yielded extremely significant results in its analysis. If implemented throughout Cyber Protection Teams, enhanced operator performance has the potential to impact cyber security on a global scale.

Acknowledgements

This material is based upon work supported by the Cyber Technologies Office of the Under Secretary of Defense Research and Engineering.

References