Careers in Play

November 2020 Newsletter
Project Update for NSF Award **1915563**

Multi-Institutional Weekly Reading Group

Every Wednesday evening, students and professors from Indiana University and the University of Maryland meet virtually to take part in a reading group centered on research relevant to Careers in Play. Each member of the reading group is responsible for selecting at least one article that they believe would enrich the theoretical understanding, design, or measurement of the different dimensions of the Careers in Play project. So far the topics have been from a diverse range of fields, from disaster response to the learning sciences, covering topics as varied as, simulations, epistemic networks, learner-centered design, and online collaborative writing.

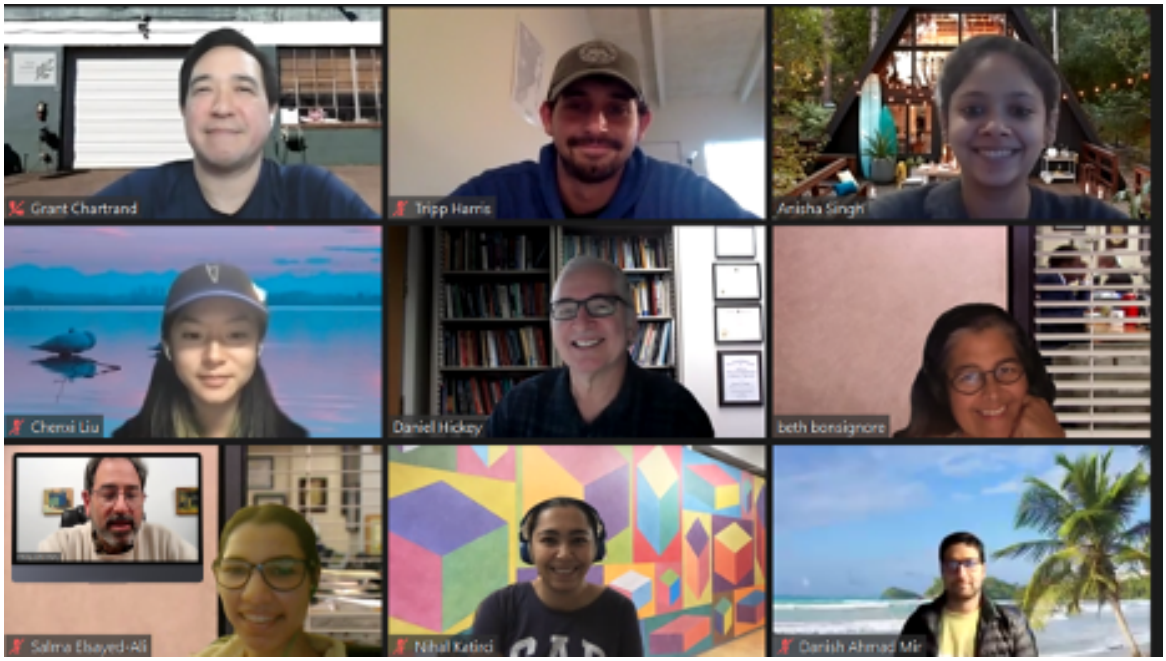

Figure 1. One of the Virtual Meetings of the Reading Group

Cybersecurity Playtesting Update

Before winding down for Thanksgiving and heralding the beginning of the holiday season, the team ran a full playtest (all but the final activity) of the Cybersecurity Playable Case Study (PCS). Although we have playtested the risk assessment activity and the cybersecurity attack activity as "stand-alone" events several times over the late spring and summer, this playtest marked the first time that undergraduate students were steeped in the interactive storyline and overarching PCS interface. Playtesting with students has given us valuable insights into what works and what areas need revision.

Puzzle Design to Promote Collaboration

First, the single activity playtests (conducted May – October) allowed us to prompt higher levels of collaboration and improve our scaffolding of disciplinary content. For example, in the risk assessment activity, a cyber incident "Breach Report" is used to help players identify current cyber threat trends. The Breach Report was initially given as a comprehensive document to all players (as a group). Through playtesting, we observed that this format inspired

little collaboration across the various cybersecurity team roles. As a result, we divided the breach report into segments, with each part highlighting the expertise of a specific role but no one segment providing enough detail to complete the risk assessment without coordination among all roles. For example, the System Administrator received trends and details regarding ransomware, while the Public Information Officer (PIO) received data on phishing attack trends and the value of training staff. In classic "jigsaw" collaboration fashion, the risk assessment tool required each player role to contribute their specific expertise from these individual components, and then weigh options together, or the team would **not** realize an optimal budget. After this relatively minor, but critical adjustment, we found that players asked each other what data they had received, discussed their component parts, negotiated with each other to achieve common ground, and developed a comprehensive risk assessment budget they could all agree would improve the fictional city's security posture. This finding also influenced and improved the cybersecurity attack activity. In many ways, our current activity format is similar to classic logic puzzles that require each player to contribute a meaningful piece that only that player can provide in order to triangulate on a final solution.

For two weeks in mid-November, we took what we had learned in the standalone activity playtests and put them together into a "full" alpha version of our PCS interface. The PCS was play-tested by 17 freshman (undergraduate) students in an introductory Information Science course (three teams of four players; one team of five). Over five class periods (~75 minutes per class), students assumed roles in the interactive narrative and completed activities as part of a fictional Professional Development Program (ProDev) for a municipal cybersecurity department in the fictional city of Bronze Falls. Students played through four virtual days as Junior Associates in Bronze Falls' ProDev Program, collaborating on three team activities: Cyber Risk Assessment, Cyber Incident Response, and Incident Attribution.

Cybersecurity Classroom Playtest

This full PCS playtest signaled the first time that students selected their own roles rather than being randomly assigned to a role for a standalone activity. First, students learned about the roles by reviewing documentation and watching videos by non-player characters (NPCs) who represented various cybersecurity-related leadership positions. Then, in true Productive Disciplinary Engagement/Expansive Framing (PDE/EF) fashion, each player submitted a personal rationale, positioned as an informal "job application," to explain why they were particularly suited for a specific role – or not. Our hope was to evaluate the interactive ways that we present these cybersecurity-related careers to students and to determine how "in-game" integrated PDE/EF assessments might work. The small cadre of freshmen seemed to enjoy learning about the various roles and applying for the positions that they felt suited them best. The short rationales provided by each student were personal, and in many cases, tied directly to the skill sets that they believed were key characteristics of the specific roles. For example, one student "applied" for the various roles as follows:

> *"I am not the best at communication and do not have very creative ways to be an effective bridge between two parties which is why I'm **least** suited to be a Public Information Officer.*
>
> *Although I am a problem solver I would much rather do software work than mechanical work which is why a Scada technician is my **third** option.*
>
> *I do well at analyzing situations, troubleshooting and finding solutions to problems which is why System Administrator is my **second** option.*
>
> *I know how to work under pressure and have a good eye for analyzing, maintaining and monitoring data so a Security Analyst would be the **best** position for me."*

Once their roles were assigned, players were divided into balanced teams and took on their first team task: the risk assessment activity that we had play-tested as a standalone throughout April-May 2020. For the most part, students were able to complete this task and negotiated amongst themselves as hoped (i.e., contributed their respective data and negotiated a comprehensive security budget). However, the PCS user interface itself had several bugs that the

design team had to work through, which caused several delays during the in-class portion of the activity. Students completed the activity as homework. While do-able, students noted that they would have preferred to collaborate in a more synchronous, in-class fashion. Below are specific excerpts from student reflections on this first activity:

> **<Student 1 (SCADA Tech)>:** *"I believe I did an average job advocating for my department as it was the 1st highest out of the 4 areas. I could have done better to get it to get more funding but the amount my department got made more sense for the benefit of everything else. Everyone else did a good job as well but one person stood out and his department a good amount of funding.*
>
> *I learned that being a SCADA technician was very important, probably one of the more important jobs out of the four. This is because of the installation and management of SCADA technology and being able to problem-solve to prevent malware attacks. As for the other jobs, I found the system administrator is very important as they had to be the one who overviews everyone to make sure everything is running smoothly. They needed to focus on being the leader and helping everyone down the right path."*
>
> **<Student 2 (SysAdmin)>:** *I think I advocated well for the needs of my department as I plugged in numbers that I assessed were right from the email I received about ransomware. I believe the rest of my junior associate team did as well. I learned more about the importance of preventing malware attacks. I learned about ransomware and how paying the ransom won't always ensure the malware still isn't there."*
>
> **<Student 3 (PIO)>:** *I felt that I advocated very well for my position of Public Information Officer for displaying my concerns about Phishing in the group. I pushed the importance of this in every aspect of our decision making process, and how it could be implemented into the overall roles of everyone in the project. I have always felt that human resources is a crucial part of any company, I felt that this position definitely connected to this role. Overall, good collaboration and employee culture is a very big component of any business, and I felt I emphasized this throughout the project. This connects to how Phishing addresses fraud scams by incorporating employee protection systems.*
>
> *Overall, my teammates also did a decent job of pushing their positions. I felt once we started working everyone knew a lot about their roles and emphasized key points in every decision we made relating to their job. Since I wasn't as knowledgeable in the IT department, I think all of them in this role excelled and had a lot of good ideas that I wouldn't have considered."*
>
> **<Student 4 (Security Analyst)>:** *"I believe that I did a good job being able to advocate for my department because I carefully read over the email that I got from my supervisor and I took into account the numbers for last year's web attacks. I played around with different numbers that I believed would be the best to include in the assessment and then I played around with the different packages that were available for the Web attacks which include bronze, silver and gold. I chose the one that gave me the best balance of a good budget that allowed for room for the other sections and I believe gave my team and department the best protection.*
>
> *Along with my team, I believe that they all thought about what would be the best option for their departments and that also gave room for the other components that we needed to include in the risk assessment and that made sense based of their information.*

Although this first "complete playthrough" playtest included more software and interface glitches than we had hoped for, most students seemed to enjoy the PCS overall. In particular, the cybersecurity attack phase was repeatedly reported as exciting.

As expected, we also noted typical classroom management issues from our design decision to situate collaborative activities as synchronous, "whole team" events. For example, in one class session, two students (from two different teams) were absent. This was during a key activity: the cybersecurity attack. One team was able to continue without its absent member, because it was a team that had been designed to have two, rather than one Security Analyst (the one 5-person team). This was a situation we had planned for: when class size does not divide evenly into multiple four-person teams, we had decided to double-up the Security Analyst role, as this role arguably requires more cybersecurity background from the outset. This team continued with the cybersecurity attack phase, although it was missing its second Security Analyst. The second missing student, a SCADA Technician, was an issue that we had

expected, but did not account for prior to this beta-test. Although we had discussed this potential eventuality in design meetings, we had only made time to design for the "extra" Security Analyst," not an absent student during a synchronous activity.

We need to better plan for these types of scenarios. Several ideas are under consideration to grapple with this in a manner that does not diminish the experience of the remaining students. One idea is to combine two roles which have the same function and let a student toggle between roles. This may be a "tidy" solution but could increase cognitive load and reduce "fun" and engagement. Another solution being considered is to have a teacher's assistant or instructor step in. This will only be viable if a limited number of groups have dropouts. The last and perhaps the most life-like solution would be to let the student group take the hit. While this action has potential to demotivate students, it is also the most realistic. The PCS would then need to account for missing students at the start of the activity. Currently, the PCS only advances to the cybersecurity attack if each role on a team acknowledges that they are "Ready," which is a common feature in multi-player mission-based games. This could be accounted for by allowing an instructor to start the activity for a team, regardless of whether all members are present.

Overall, we have learned a great deal from our first, two-week run through, and have ironed out several software issues, as well as updated several narrative elements. In addition to formalizing contingency plans for missing students during synchronous PCS activities, we will be working out the interface kinks for several more weeks to ensure that the full version is production ready for the spring semester. We look forward to having our Advisory Board also playtest the "full" PCS, despite its current "alpha-beta" prototype design. We look forward to reporting on their December 7th playtest in our next newsletter.

Upcoming Conference Symposium

This summer we put together a symposium that brings together scholars researching how textual practices promote learning and engagement in different disciplines. The symposium proposal was submitted to the American Educational Research Association and has been accepted to be presented at their annual conference to be held in April 2021. The symposium is entitled: *Productive Disciplinary Engagement and Textual Practices.*

We will be providing more details about the sessions as we get closer to the date in our subsequent newsletters.

Team Member Spotlight: Grant Chartrand

Grant is a fourth-year PhD student in Learning Sciences at Indiana University. In Careers in Play (CiP) he works closely with Dan Hickey to develop effective assessments. He is also an active member of CiP's literature review team. Grant has extensive experience with urban planning in general and disaster preparedness in particular. He is lending his expertise to the disaster response design team as they work toward creating an engaging PCS. If this were not enough, Grant is also the lead facilitator of the reading group. Grant's research and scholarly interests are in online, asynchronous learning, design theory and practice, and sociocultural theories of learning.

Careers In Play Leadership Team

Phil Piety, PhD. University of Maryland iSchool (PI and Learning Analytics). ppiety@umd.edu

Beth Bonsignore, PhD. University of Maryland iSchool (Co-PI and Design-based Research), ebonsign@umd.edu

Derek Hansen, PhD.Brigham Young University (Co-PI and Game Technology). dlhansen@byu.edu

Dan Hickey, PhD Indiana University School of Education (Co-PI, Learning Theory and Assessments). dthickey@umd.edu

COLLEGE OF INFORMATION STUDIES

BYU | IRA A. FULTON COLLEGE ENGINEERING AND TECHNOLOGY

INDIANA UNIVERSITY SCHOOL OF EDUCATION