Human Behavior Analytics from Microworlds: The Cyber Security Game

Johan de Heer(✉) and Paul Porskamp

Thales Research and Technology T-Xchange, University of Twente,
Westhorst Building 22 – WH226, Drienerlolaan 5,
7522 NB Enschede, The Netherlands
{Johan.deHeer,Paul.Porskamp}@nl.thalesgroup.com

Abstract. Games viewed as socio-technical representations of real world system-of-systems may turn into Microworld research tools to monitor human dynamic decision making. In this paper we illustrate the potential of this methodology focusing on a Cyber Security Dilemma game, and various player models that we can elucidate from them at individual and aggregated levels.

Keywords: Game based learning · Stealth assessment · Human behavior modelling · Cyber security

1 Introduction

Making judgments and taking decisions is daily practice for lots of people. Understanding and elucidating the dynamics of human reasoning, however, is an enigma and requires a theory of mind, appropriate theoretical concepts, methods and techniques for studying Dynamic Decision Making (DDM). Let alone, predicting human judgment and decision-making behaviors. This paper sketches a '*game-based-micro-world*' for studying Dynamic Decision Making [1]. Microworlds [2] are used to record, monitor and analyze how people make decisions over time. DDM takes into account [3]: sequences of decisions to reach a goal, interdependence of decisions on previous decisions, dynamics of a changing environment, and that decisions are made in real time (that is, in time pressured situations). We illustrate such a microworld with an example that enables us to study how players in the role of crisis managers make decisions during the unfolding of a cyber security interactive storyline. In addition, we present several type of human behavioral models, including risk taken and avoidance behaviors that can be provided by game statistical and analytical services.

2 Microworld: Cyber Game

We designed and developed a game based microworld (see Fig. 1) that represents the essential real world elements during a cyber crisis from the crisis manager point of view. Note, that it is beyond the scope of this paper to discuss how we designed and developed this model-based and configurable game based microworld. It needs understanding of the

D. Nicholson (ed.), *Advances in Human Factors in Cybersecurity*,
Advances in Intelligent Systems and Computing 593, DOI 10.1007/978-3-319-60585-2_17

Fig. 1. Single player turn taking 2D narrative game.

specific game scenario [4], how to design a game based systems [5], and a thorough understanding of the components that game systems are made of [6].

The game flow of this single player turn-taking narrative game based microworld is as follows. First, the crisis manager – the player - is presented a context scenario, in which the setting is briefly explained (Fig. 2), in this case the occurrence of a petrochemical disaster.

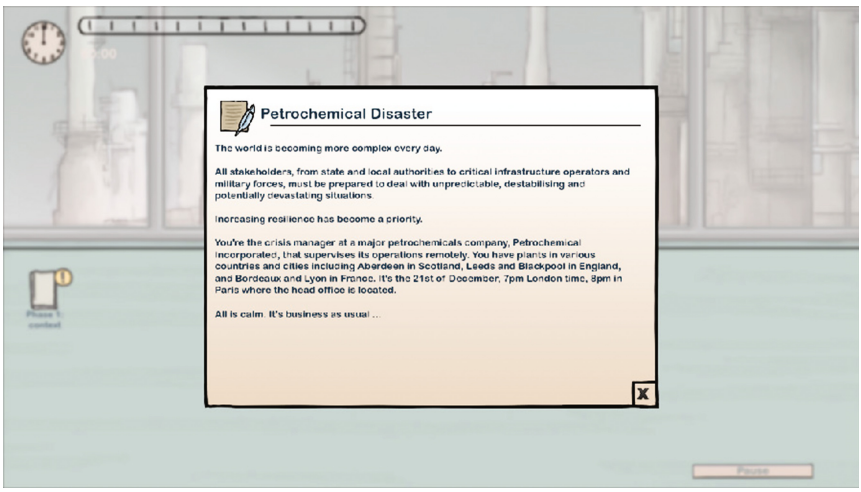


Fig. 2. Context scenario

Related to this context scenario, a series of six dilemmas are introduced that all end with a question where the player has to make a 'yes' or 'no' decision. The dilemmas – depicted in bottom left corner in the form of envelopes can be opened with a simple mouse click - appear over the course of (playing) time (Figs. 1 and 3). A typical dilemma relates to aspects of uncertainty and ambiguity of a specific crisis phase. The decision to take is for example: 'Do you activate the business continuity plan at this stage?' Note, that this game based microworld embeds dilemmas where there is no right or wrong answer; for each decision a rationale may be found, or a story can be told or argued. In the game (virtual) crisis team members are gathered around a table and may let the player know if they have potential relevant information (depicted by a text balloon above their heads) that may possibly alter the decision - if taken into account by the player. There are the CEO, the operations manager, the communication manager, the legal affairs manager, the Business Continuity Manager, the IT manager of the company, and even a representative of the national security agency, called in because of the unusual nature of the crisis [4]. The player is free to select and read information from his team advisors, and may even ask them for advice what they would decide - indicated by green (voting for a yes decision) and red (voting for a no decision) (Fig. 3).

Fig. 3. Asking information and/or advice

Once, the dilemma has been answered, the game pauses and the player is asked to indicate, which information provided by a virtual team member was taken into account and considered relevant regarding the decision s/he took. Virtual characters start to smile after a while if the player occasionally 'listens' to them, but will look sad if players just 'hear' what they have to say. Secondly, the player needs to indicate his/her perception with respect to the impact of the decision on the customers, internal staff or the general public (see Fig. 4). After the player provides this in-situ input, the player automatically returns to the game.

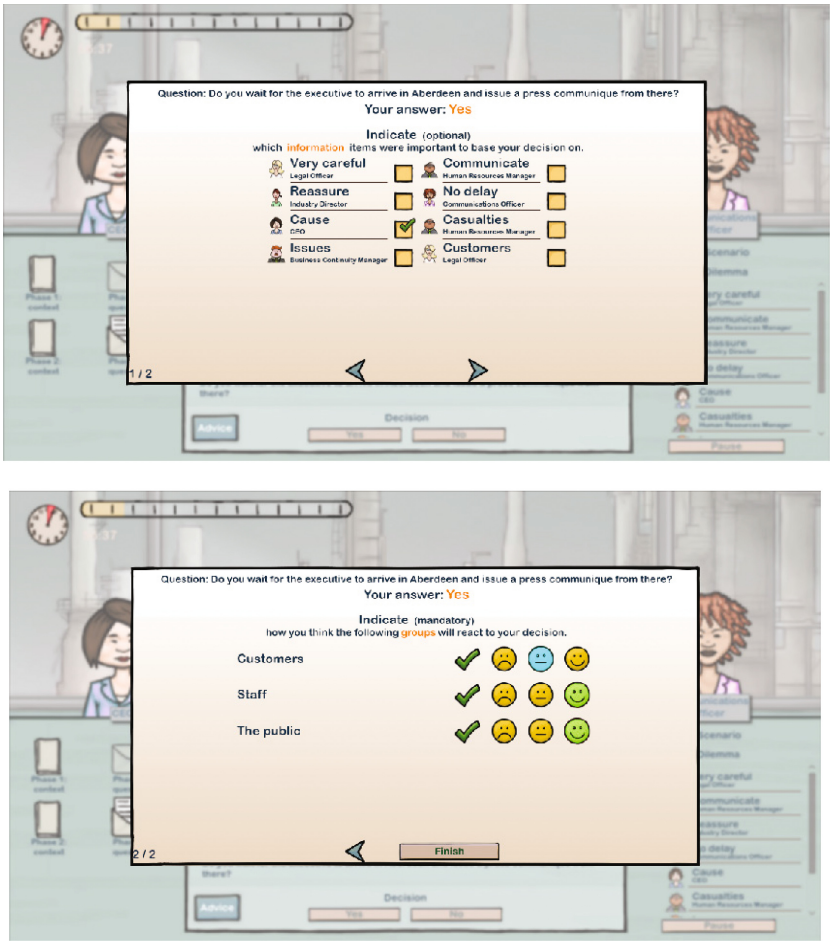


Fig. 4. In-situ input

The game ends when all dilemmas have been answered. The player may read all information items, and even advices what to decide from his/her team members, but it is up to the player to decide if and when s/he uses this information.

3 Game Statistics

First, we generate simple descriptive statistics about the time needed to answer dilemmas, the number of dilemmas answered, the number of times advices of various team members were indicated as important (Fig. 5). This is done on an individual level and provided as feedback to the player. Further analysis is done on aggregating levels based on all game log-files.

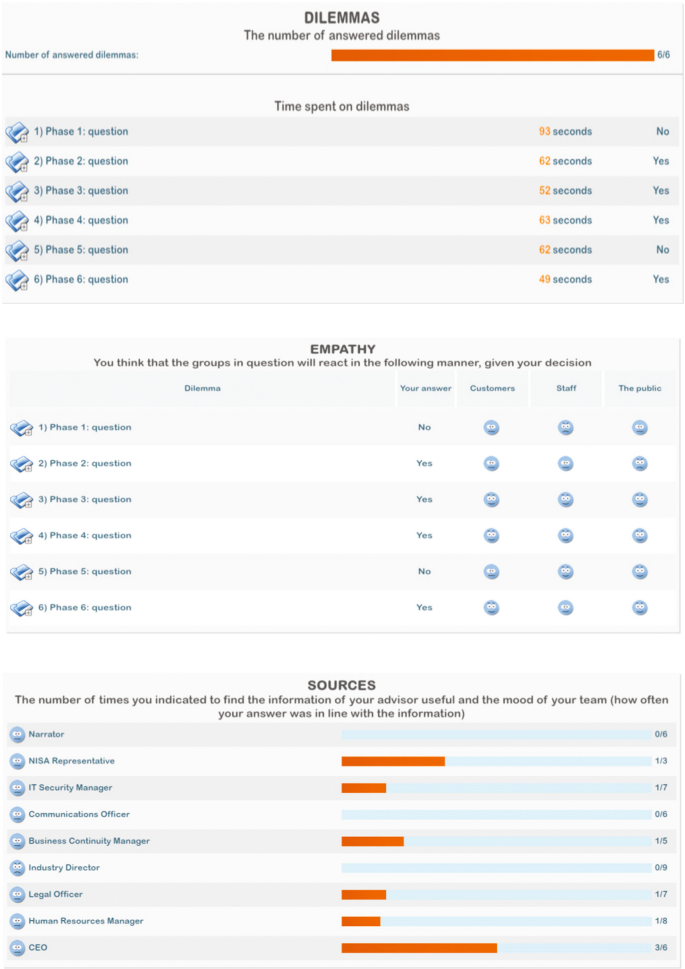
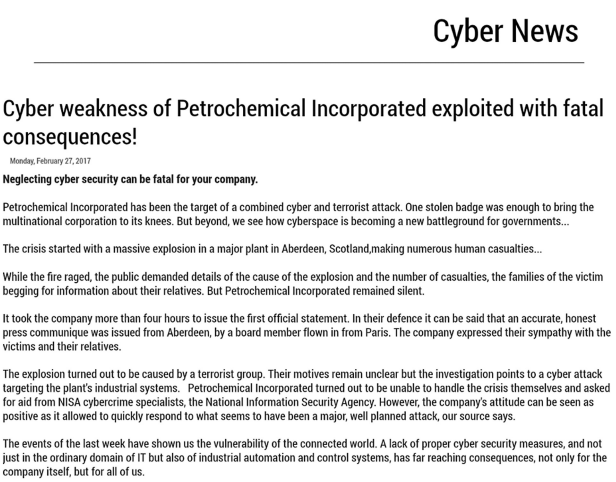


Fig. 5. Game descriptive statistics

Second, we generate a newspaper article where the narrative is based on the choices the player made during gameplay (Fig. 6).


Cyber News

Cyber weakness of Petrochemical Incorporated exploited with fatal consequences!

Monday, February 27, 2017

Neglecting cyber security can be fatal for your company.

Petrochemical Incorporated has been the target of a combined cyber and terrorist attack. One stolen badge was enough to bring the multinational corporation to its knees. But beyond, we see how cyberspace is becoming a new battleground for governments...

The crisis started with a massive explosion in a major plant in Aberdeen, Scotland,making numerous human casualties...

While the fire raged, the public demanded details of the cause of the explosion and the number of casualties, the families of the victim begging for information about their relatives. But Petrochemical Incorporated remained silent.

It took the company more than four hours to issue the first official statement. In their defence it can be said that an accurate, honest press communique was issued from Aberdeen, by a board member flown in from Paris. The company expressed their sympathy with the victims and their relatives.

The explosion turned out to be caused by a terrorist group. Their motives remain unclear but the investigation points to a cyber attack targeting the plant's industrial systems. Petrochemical Incorporated turned out to be unable to handle the crisis themselves and asked for aid from NISA cybercrime specialists, the National Information Security Agency. However, the company's attitude can be seen as positive as it allowed to quickly respond to what seems to have been a major, well planned attack, our source says.

The events of the last week have shown us the vulnerability of the connected world. A lack of proper cyber security measures, and not just in the ordinary domain of IT but also of industrial automation and control systems, has far reaching consequences, not only for the company itself, but for all of us.

Fig. 6. Generated newspaper article

Third (see Fig. 7), the players' decisions are related to two different risk taken vs. risk avoidance dimensions, 'risk taken/avoidance behaviors regarding reputational risks' and 'risk taken/avoidance behaviors regarding operational risks'. Reputational risks, often called reputation risks, are risks of loss resulting from damages to a firm's reputation. Operational risks are risks of loss resulting from inadequate or failed internal processes, people and systems or from external events. The scoring is based on an in-game algorithm defined by a subject matter expert with domain knowledge [4, see also acknowledgement].

Fig. 7. Risk reputational/operational leadership style

4 Game Analytics

The individual game log data files can be further analyzed into meaningful information to shed light on human reasoning aspects. This makes it possible to examine team and group behaviors across a number of other parameters as well e.g., level of expertise, gender, country, culture, business domain, etc. That activity is still underway and experiments conducted and data gathered will be addressed in future papers. In the following, we are basically pointing to methodological aspects, and the sorts of data

and informational patterns we can get out of this type of microworld. We will not provide psychological nor economical interpretations of the statistics and analytics at this point[1].

The analytics provided here are based on the Cyber Security game (cis.txchange.nl) that ran on-line between 2015–2017. The game was accessible on the internet and over this period played 887 times. The web-based game is available in two languages: English and French. Figure 8 show the number of times the game is played across this timespan.

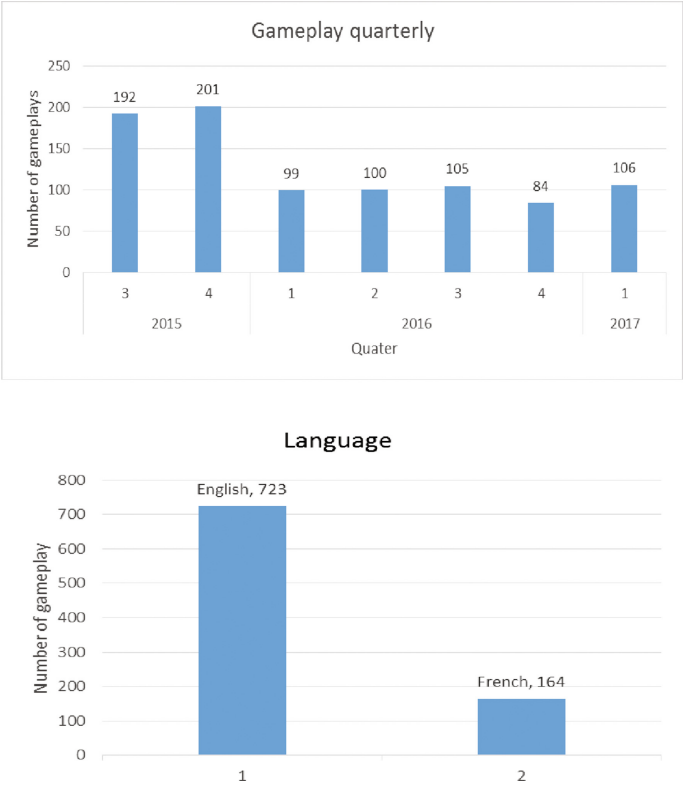


Fig. 8. Total number of game plays over time and between two game variants (English and French version)

For analytical purposes we selected a dataset out of the total of 887 game log files available. We assumed that not all 887 games were played 'seriously'. We consider a seriously played game when (1) at least 4 out 6 dilemmas were answered, (2) at least for 3 dilemmas minimal 2 information items were opened, (3) that the game play duration at least 7 min took but not longer than 35 min. Thus, a 'seriously' played

[1] To falsify your own hypotheses and utilize the data files please contact the authors of this paper.

game utilizes all available game mechanics for several times. Based on these selection criteria we ended up with 377 (out of 887) seriously played games with an average playing time around 10 min. We used these 377 game loggings for further visual inspection and analyses.

Figure 9 illustrates the overall scoring with respect to the playing styles. Reputation risk taking 42% vs. Reputation risk avoidance 58%, Operation Risk taking 29% vs. Operation risk avoidance 71%. These figures are in line with the negativity bias in a plethora of situations related to risk-averse behaviors. Operational risk is the risk arising from execution of a company's business function. And, focuses on the risks arising from people, processes, and systems, including external events that affect a company's operations. Our data indicate that those who played the game are more risk averse regarding operational - than reputational issues. Reputational risk may arise from operational risk but is not, in and of itself, an operational risk.

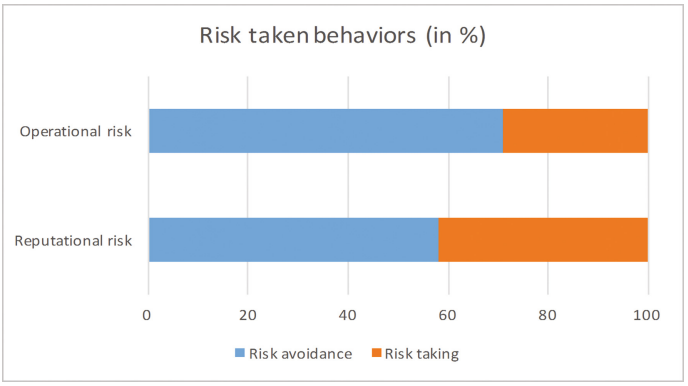


Fig. 9. Risk taken vs. risk avoidance behaviors regarding operational and reputational risks

Figure 10 shows that all scores significantly differ from the 50% change level; using the Nonparametric one-sample Binomial test (significance level is 0.5).

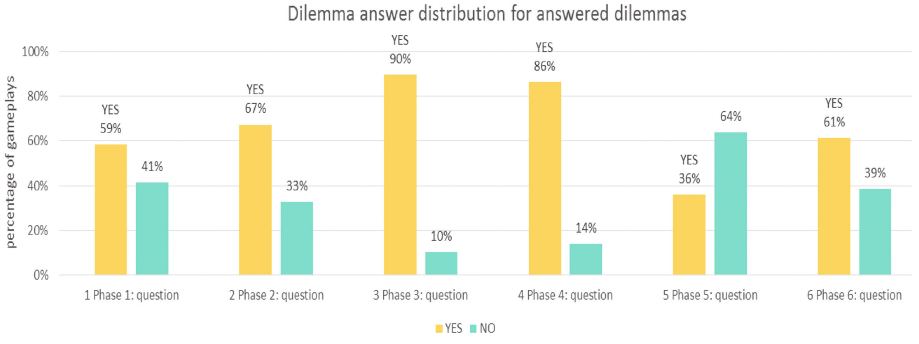


Fig. 10. Yes/no distribution across dilemmas

Figure 11 illustrates the difference in risks behaviors across the different phases during the crisis. The first phase characterized the beginning of the crisis, in the second phase the crisis starts to get going, in the third phase it escalated to reach its climax in the fourth phase, in the fifth phase the company was no longer to target of cyber attacks and the crisis was really over in de sixth phase. In addition, the average decision times for all dilemmas are depicted as well. Note that the no data/scoring was available for reputational risk for the third dilemma.

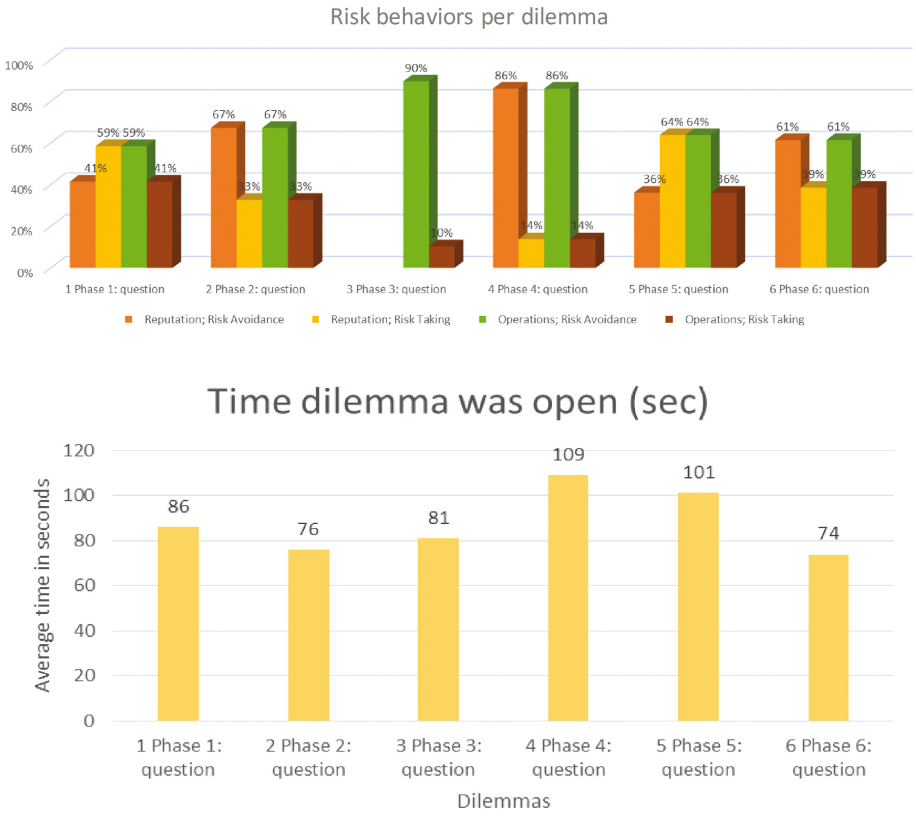


Fig. 11. Risk behaviors and decision-making times per dilemma

Figure 12 shows the percentage that an information item provided by a specific virtual character sitting at the table is opened (in red) and considered important (in blue) by the player. Immediately below the graph regarding the total percentages across the dilemmas.

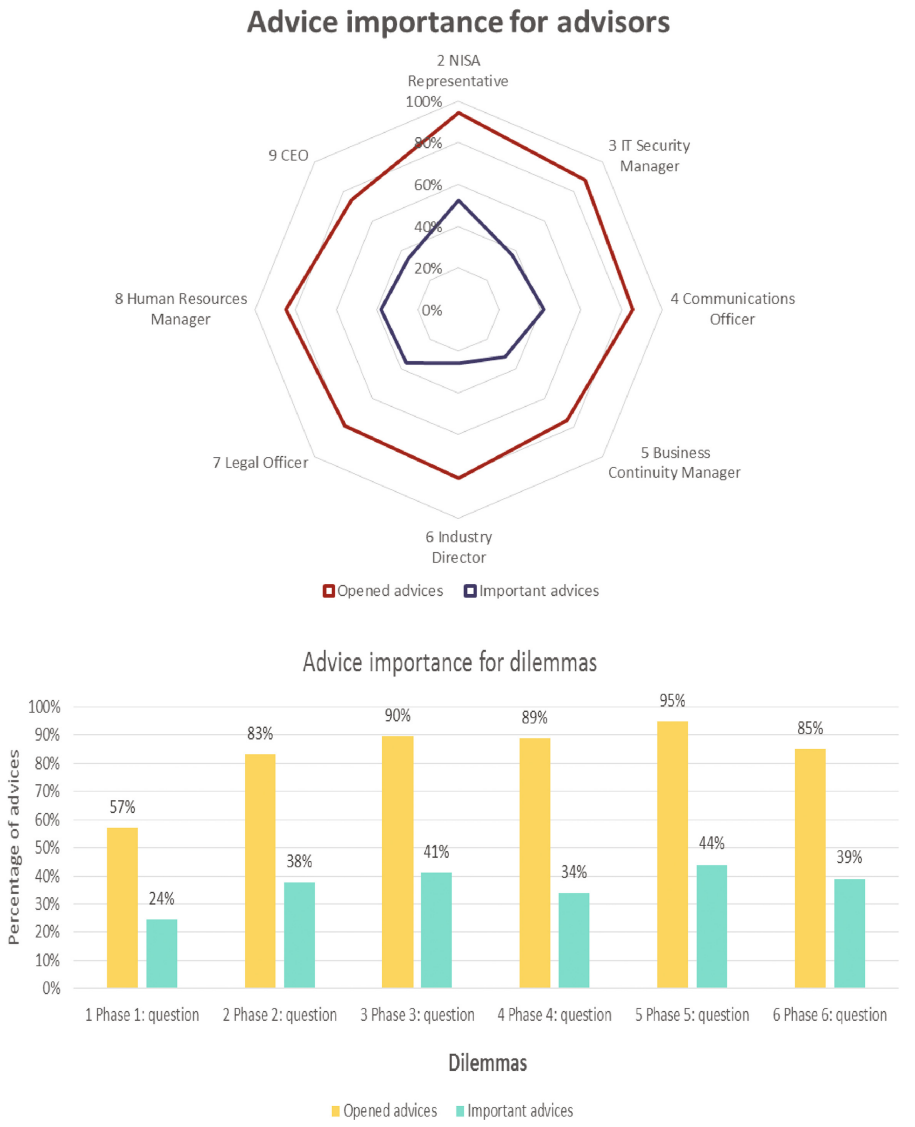


Fig. 12. Advices by virtual characters

Finally, Fig. 13 depicts how many times (in percentages) the player asked for a voting advice (yellow graph) and the times they followed (implicitly) the voting advices by the virtual characters. And in the figure underneath, the average voting advices per dilemma.

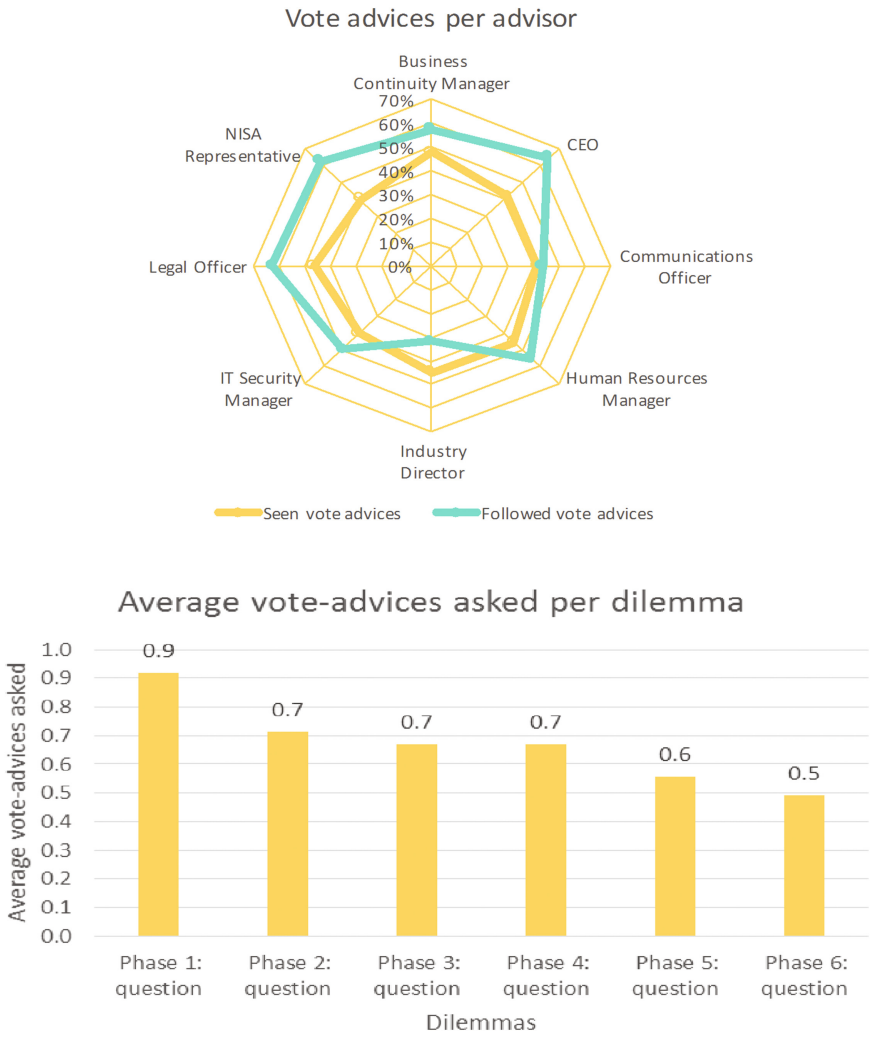


Fig. 13. Voting advices

5 Conclusion

The general goal the present paper was to show that microworlds can provide data and information that can be used for elucidating dynamic decision making models. This was illustrated by risk behaviors during a Cyber attack. We conclude that game based microworlds will bring us statistic and analytics in understanding how we think, reason, and decide. This type of data can be used by researchers to falsify their hypotheses. For example, related to research questions on the type and occurrence of risk behaviors during several crisis situations. Our future work is focusing on the unobtrusive measurement of competency where we explore the combination of several

top-down (e.g. Bayesian networks) and bottom-up data mining techniques to analyze and predict human behaviors. We not only focus on competencies but also on preferred playing styles during game flow, in terms of actions, tactics, and strategies for managing the uncertainty and dynamics in the game [7, 8]. The latter is important, since player strategies are suggested as predictors regarding transferability from in game to out of game behaviors [9].

Acknowledgments. The game scenario was developed with Paul Théron [4] a Thales cyber security expert.

References

1. De Heer, J.: How do Architects think? A game based microworld for elucidating dynamic decision-making. In: Auvray, G., et al. (eds.) Complex Systems Design and Management, pp. 133–142. Springer International Publishing, Cham (2016). doi:10.1007/978-3-319-26109-6_10
2. Brehmer, B., Dorner, D.: Experiments with computer simulated microworlds: escaping both the narrow straits of the laboratory and the deep blue sea of the fields study. Comput. Hum. Behav. **9**, 171–184 (2003)
3. Gonzalez, C., Lerch, J.F., Lebiere, C.: Instance-based learning in dynamic decision making. Cogn. Sci. **27**, 591–635 (2003)
4. Théron, P.: Informing business strategists about the cyber threat: why not play serious games? In: Hills, M. (ed.) Why Cyber Security is a Socio-Technical Challenge: New Concepts and Practical Measures to Enhance Detection, pp. 129–158. Northampton Business School, University of Northampton, UK (2016). ISBN 978-1-53610-090-7
5. Klabbers, H.G.: The Magic Circle: Principles of Gaming and Simulation, 3rd edn. Sense Publishers, Rotterdam (2009)
6. Schell, J.: The Art of Game Design: A Book of Lenses, 2nd edn. AK Peters/CRC Press, Natick (2008)
7. Bakkes, S.C.J., Spronck, P.H.M., van Lankveld, G.: Player behavioural modelling for video games. Entertainment Comput. **3**, 71–79 (2012)
8. Ross, A.M., Fitzgerald, M.E., Rhodes, D.H.: Game-based learning for system engineering concepts. In: Conference on Systems Engineering Research, pp. 1–11 (CSER 2014) (2014)
9. Kaser, T., Hallinen, N.R., Schwartz, D.L.: Modeling strategies to predict student performance with a learning environment and beyond. In: Proceedings of the Seventh International Learning Analytics and Knowledge Conference, LAK 2017, pp. 31–40 (2017). ISBN 978-1-503-4870-6