Successful gamification of cybersecurity training

Steen, T. van; Deeleman, J.R.A.

CYBERPSYCHOLOGY, BEHAVIOR, AND SOCIAL NETWORKING
Volume 00, Number 00, 2021

DOI: 10.1089/cyber.2020.0526

Successful Gamification of Cybersecurity Training

Tommy van Steen, PhD[1,i] and Julia R.A. Deeleman, MSc[1,2]

Abstract

The behavioral aspect of cybersecurity has gained more attention in recent years. By their actions, people can improve the security of their devices and organizations, but also hinder the successful implementation of security in these areas. As awareness campaigns where information is merely distributed are not effective, we designed a cybersecurity serious game applicable for cybersecurity training. The effectiveness of this game was experimentally tested against a noncybersecurity game that did or did not contain cybersecurity information, through measures of the theory of planned behavior. Results showed that the cybersecurity game resulted in higher self-reported scores on attitudes, perceived behavioral control, intentions, and behavior compared with both noncybersecurity games. For subjective norms, we only found an effect in the comparison between the cybersecurity game and the noncybersecurity game without additional information.

Keywords: behavioral cybersecurity, cybersecurity training, gamification, serious games, theory of planned behavior, behavior change

Introduction

THE CONSEQUENCES OF CYBERATTACKS are often severe. Data breaches or hacks have the potential to cause major economic or reputational damage, reducing trust in the attacked organization.[1] Furthermore, even the data of individual users are not safe, and the consequences of cyberattacks are widespread and cause potential threats to national security.[2] Besides technical solutions, the focus lies increasingly on cybersecurity training for end-users. Various approaches exist, ranging from widespread, but not very effective, awareness campaigns[3]; challenge-based learning, in which participants receive multiple challenges on specific domains[4]; capture the flag events, in which participants are to secure their flag or file and capture those of others[5]; or tabletop games.[6]

Another approach is to implement a serious game. A serious game differs from a regular game in that serious games do not have the primary purpose to entertain or provide enjoyment.[7] Instead, serious games aim to facilitate learning among participants.[8] Besides this educational goal, they can be designed as activities, taking place at a certain time and location, and which have certain rules attached.[7] Serious games can be used to train or educate an audience through interactive elements in the game that are either explored alone or with others. Serious games can be more effective in expanding knowledge and cognitive skills in comparison with regular instructional approaches.[9]

Applications of serious games in the cybersecurity sphere can range from wargames[10] to safety and security games, which are a good alternative to regular safety training and allow learners to consider different scenarios before encountering them in their daily lives.[11] A structured literature review concluded that cybersecurity might be a suitable topic for providing training through serious gaming.[12] The authors analyzed games, such as mobile and three-dimensional virtual world games, which focused on a range of topics, including cybersecurity awareness, phishing, and network security. They suggested that security in these areas can be improved by using serious games to train people. However, the authors note that sample sizes were often small and they call for more robust evaluations of cybersecurity serious games in the future.[12]

This study investigates whether a serious game that is designed based on the findings of previous studies and best practices can improve participants' scores on theory of planned behavior (TPB) factors.[13] The TPB suggests that behavior is the result of an interplay between a person's attitudes (Do they value cybersecurity?), social norms (Do they perceive their environment to be secure and does

[1]Institute of Security and Global Affairs, Leiden University, The Hague, The Netherlands.
[2]L.I.B. Businessgames, Breda, The Netherlands.
[i]ORCID ID (https://orcid.org/0000-0002-5805-4664).
The study was carried out as an MSc thesis in Crisis and Security Management at Leiden University.

the environment value security?), perceived behavioral control (Do they feel confident they can perform the behavior?), and intentions (Do they intend to perform the security behavior?). The TPB is a useful model for conceptualizing serious gaming in the context of cybersecurity as it takes into account not only personal attitudes, but also the influence of peers and perceptions of ability, allowing us to investigate more than just the change in intentions or behavior. If the serious game does not affect the behavioral intention, measuring all TPB elements can provide insight into which underlying factors require further investigation in future research.

Previous research on serious games in other fields showed that they are effective in training participants. For example, serious games can improve skills regarding safe sex negotiations through an adventure game.[14] Furthermore, game-based entrepreneurship education has been shown to have a positive influence on behavioral intentions.[15] Finally, serious games were successful in reducing energy consumption behavior.[16,17] Nevertheless, serious games have not yet proven to be successful in leading to a positive change in perceived behavioral control or subjective norms.[18,19]

Given that no research has yet been conducted into the effectiveness of serious games on the TPB predictors of cybersecurity behavior, and no study has yet investigated the effectiveness of serious games on all TPB factors, this study attempts to fill this gap in the literature. Building upon previous research, it is hypothesized that compared with playing a control game that does, or does not, include a poster with cybersecurity information, playing a cybersecurity serious game will cause a positive change in all TPB predictors of cybersecurity behavior: (H1) attitudes toward cybersecurity; (H2) subjective norms regarding cybersecurity; (H3) perceived behavioral control related to cybersecurity; and (H4) behavioral cybersecurity intentions.

Materials and Methods

Participants and design

The Institute of Security and Global Affairs' ethical procedure for student projects was followed, where students complete an ethics survey about their project and any issues that are flagged as a result of completing this survey are discussed with their supervisor and resolved before data collection. Since the risks to the student researcher and research participants were deemed sufficiently minimal, formal Institutional Review Board approval was not required.

Participants were recruited through social media accounts whose owner is located in Netherlands (Instagram and Facebook), e-mail, and a company networking service (Yammer). A link to participate in the cybersecurity game was shared on these platforms. Snowball sampling was used in the recruitment process, with less than half (48.5 percent) of the participants receiving the link directly from the researchers. Although 425 participants arrived at the start of the game, 167 participants dropped out before completing the game. The remaining 258 participants (129 women, $M_{age} = 30.5$, $SD = 12.3$, employees: 53.1 percent, student: 40.7 percent, other occupation: 6.2 percent) were randomly assigned to one of three conditions (control game, control game plus information, and cybersecurity game) and completed a postgame TPB questionnaire.

Materials

Serious games. We designed two games: a cybersecurity game and a noncybersecurity cooperation game. Both games were designed using the survey platform Qualtrics. This way, participants could play the game in their own time and at their own pace. Participants would start on a single page with a game task and would be redirected to new pages with other game tasks based on their in-game choices. The primary goal of these games was to provide learning opportunities, with enjoyment as a secondary goal, in line with the general concept and application of serious games.

In the cybersecurity game, participants encountered a number of cybersecurity incidents, ranging from protecting against phishing e-mails to baiting attacks, and were taught what they could do to be more cybersecure. If they did not give the correct response to the incident, there were consequences (e.g., a lower score in the game) and participants were informed of what they should have done instead and why. This ensured that participants who did not do well learned what they should do in the future, thereby improving cybersecurity knowledge and relevant skills. In the other conditions, participants played the cooperation game that acted as control game. In this game, participants solved cooperation-focused incidents in which they were asked for help by nonplayer characters. These incidents were unrelated to cybersecurity. In the control plus information condition, cybersecurity information from the cybersecurity game was added to the cooperation game in poster format. In both the cybersecurity and control games, participants received a pot of money that they could spend during the game to buy assets and collect smileys. Providing players with resources (money) and a goal (smileys) is a common gamification element. In both games, participants were encouraged to collect as many smileys as possible. These smileys could be obtained by correctly dealing with incidents, spending money on relevant updates and not overspending their budget (See Fig. 1 for an example of how participants could spend money on updates in both the cooperation game and the cybersecurity game, and Fig. 2 for an example of an incident in the cybersecurity game). The games were designed using best practices and a variety of serious game frameworks from the scientific literature.

At the start of the game, participants created a logo and motto, as research has shown that incorporating fun elements leads to increased engagement and more successful games.[20] Others have argued that increasing the level of difficulty as the game progresses leads to a better learning experience.[21] In line with this, the game initially provided participants with useful information before each incident, but this support was removed as the game progressed.[22] Furthermore, earlier research on realism in serious games concluded that adding realism increases effectiveness,[11] and this was operationalized in our serious games by ensuring that all decisions were about existing products and services, rather than using fantasy elements. Reflecting on choices afterward has also been linked to fostering deeper interaction with the materials,[20] and has, therefore, been implemented into our serious games. The goal of obtaining as many smileys as possible was set to keep the players motivated during the game. This type of scoring system has shown to be useful as it shows the players their progress and motivates improvement.[11] See Table 1 for an overview of the incorporated game elements and structure.

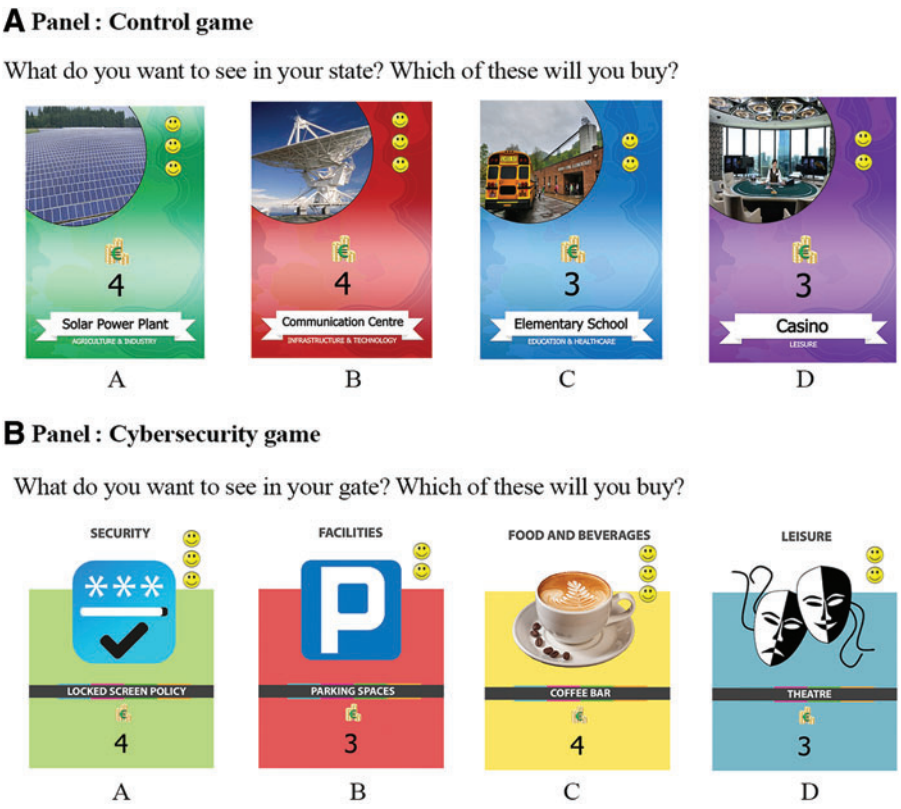

FIG. 1. Example of the game element of buying assets in the control game **(A)** and cybersecurity game **(B)**. This figure was adapted from work by L.I.B. Businessgames. Color images are available online.

TPB questionnaire. The TPB questionnaire consisted of 15 questions relating to attitudes, subjective norms, perceived behavioral control, intentions, and self-reported behavior on a 7-point Likert scale ranging from 'Strongly Disagree' to 'Strongly Agree', which were aggregated into total scores for each factor. Potential scores ranged from 3 to 21. The questions were based on TPB literature[23,24] and can be found in Table 2.

Procedure

Participants received the link to the online Qualtrics study through one of the recruitment methods mentioned earlier. Upon clicking on the link, they were directed to a landing page with a short introduction to the study and a consent form before moving on to a set of demographic questions. Participants were

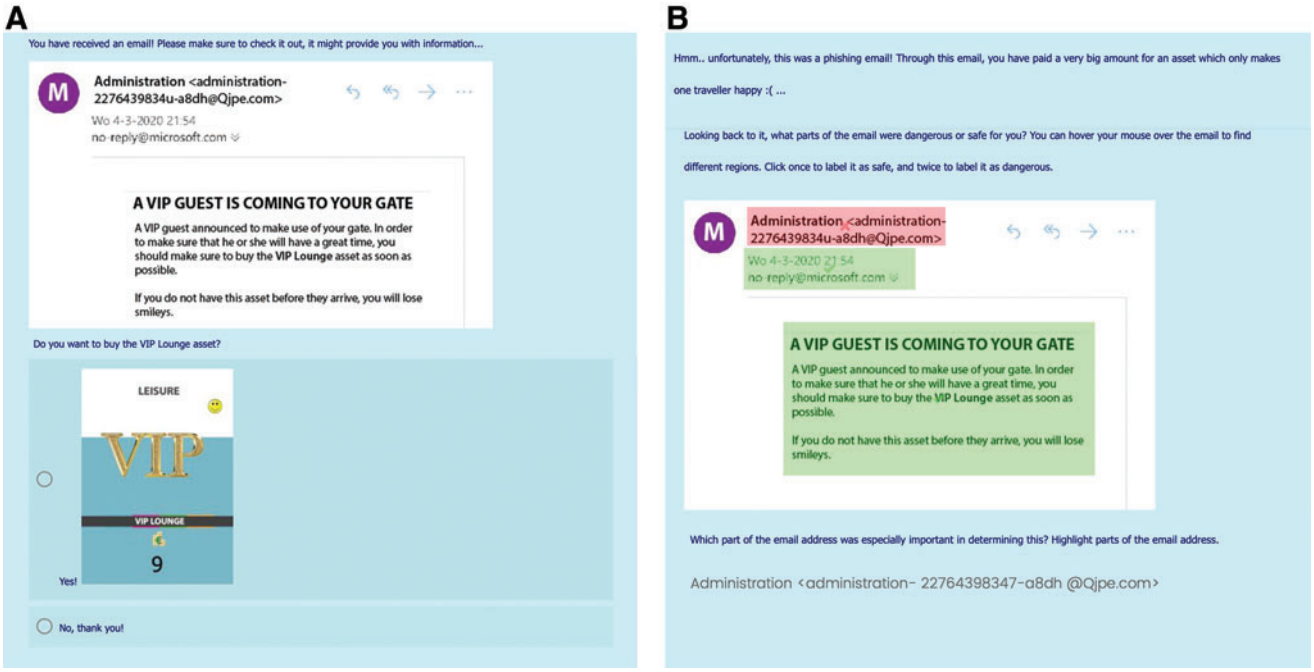

FIG. 2. Example of an incident in the cybersecurity game **(A)** and reflection after the incident **(B)**. Color images are available online.

Table 1. Overview of Game Structure and Elements

Condition	*Control game*	*Control game plus information*	*Cybersecurity game*
Game	''United Nations'' A cooperation game	''United Nations'' A cooperation game plus cybersecurity information	''The Terminal'' A cybersecurity game
Metaphor	A fictional map with six states, participant represent a state of their choice		A fictional airport with six gates, participants represent a gate of their choice
Goal	Collecting as many smileys as possible, representing happy inhabitants		Collecting as many smileys as possible, representing happy travelers
Structure	Round 1: Creating a logo for the chosen state and develop a strategy		Round 1: Creating a logo for the chosen gate and develop a strategy
	Round 2: Buying assets for their states and solve cooperative incidents		Round 2: Buying assets for their gates and solve cybersecurity incidents
	Round 3: Buying assets for their states and solve cooperative incidents		Round 3: Buying assets for their gates and solve cybersecurity incidents
Incidents	Four incidents on the following topics:		Four incidents on the following topics:
	1. Support during a military conflict		1. Phishing
	2. Neighboring states wanting to borrow money		2. Password strength
	3. Neighboring states who want to cooperate in building assets collaboratively		3. Computer updates
	4. Health care support		4. Malicious USB devices
Feedback	After every incident, participants were asked to reflect on the choice they made. After explaining their motivation, participants received feedback. Participants thus learned the consequences of cooperating (or not) or behaving in a manner consistent with cybersecure practices (or not)		

USB, universal serial bus.

then randomly assigned to one of the three conditions: the control condition with or without cybersecurity information (the cooperation game), or the experimental condition (the cybersecurity game). The games were played individually on a computer or mobile device, a factor that was not recorded to preserve participants' privacy. After finishing the game, participants completed the TPB questionnaire and were debriefed and thanked for their time. Participants did not receive any compensation for taking part in the study.

Results

Dropout rates

As 258 participants completed the study, whereas 167 participants dropped out before completion, we first examined the dropout statistics. A chi-square test showed that dropout rates did not differ between conditions [$\chi^2(2) = 2.143$, $p = 0.34$], suggesting that the type of game did not cause participants to drop out. Furthermore, we looked at the completion time. To avoid the influence of outliers, we compared the median completion time of finished games (including completing the TPB questionnaire) with the median time spent by participants who dropped out. The median duration of the finished games was 23 minutes (ranging from 21 to 25 minutes between conditions), whereas the median duration of the unfinished games was 2 minutes (ranging from 1 to 3 minutes between conditions) indicating that participants who dropped out did so early on. We, therefore, believe that the chance of a selection bias affecting our results is low.

Table 2. Theory of Planned Behavior Survey Items

TPB component	*Questions*
Attitudes	It is important to at all times adhere to cybersecurity policies
	It is important to always update computers and software
	It is important to always use antivirus to scan computers
Subjective norms	Most people around me obey to the cybersecurity policy of my company/study program at all times
	Most people around me lock their screen at all times when leaving their computer
	Most people around me update their computers at all times
Perceived behavioral control	I find it easy to ensure that I always comply with the cybersecurity policy
	I find it easy to ensure that I never open any phishing e-mails
	I find it easy to ensure that I always scan my computer
Intentions	I plan to always check received e-mails for potential phishing e-mails
	I intend to lock my screen every time I leave my computer
	I intend to always develop strong passwords
Self-reported behavior	I do my best to perform cybersecure behavior at all times
	I always check an e-mail for being a potential phishing e-mail
	I always lock my screen when I leave my computer

TPB, theory of planned behavior.

Main analysis

For the TPB predictors and behavior, analysis of variance (ANOVA) tests were run and *post hoc* pairwise comparisons were conducted taking into account multiple comparisons. The ANOVA tests showed significant differences between conditions for all TPB predictors and behavior (all p's < 0.02; see Table 3 for ANOVA statistics and pairwise comparison significance levels). No significant differences were found between the control condition and the control plus information condition on TPB predictors and behavior (all corrected p's > 0.7). Participants in the cybersecurity game scored significantly higher than participants in the control game for all TPB factors: attitudes ($d = 0.54$, 95% confidence interval [CI 0.24–0.84]), subjective norms ($d = 0.40$, 95% CI [0.10–0.70]), perceived behavioral control ($d = 0.46$, 95% CI [0.16–0.76]), intentions ($d = 0.73$, 95% CI [0.42–1.03]), and surprisingly, behavior ($d = 0.44$, 95% CI [0.15–0.74]), thereby confirming H1–H4. The participants in the cybersecurity game did not outperform the participants in the control game plus information condition on subjective norms ($d = 0.34$, 95% CI [0.03–0.64]) after controlling for multiple comparisons, but did score higher on the other TPB predictors and behavior: attitudes ($d = 0.39$, 95% CI [0.09–0.70]), perceived behavioral control ($d = 0.39$, 95% CI [0.09–0.70]), intentions ($d = 0.65$, 95% CI [0.34–0.96]), behavior ($d = 0.46$, 95% CI [0.16–0.77]), confirming H1, H3 and H4 but not H2.

Discussion

Overview of findings

Our study shows that a theory-informed serious game on cybersecurity can have a positive effect on self-reported TPB scores and behavior. Although serious games have been found to positively affect attitudes and intentions in earlier research, our study adds to these findings by showing that subjective norms and perceived behavioral control can also be influenced this way. In addition, we have shown that merely providing information does not lead to significant changes compared with a control condition. This supports the notion that informing people of best practices alone is not sufficient to create change.

Although the significant effects of condition on attitudes, subjective norms, perceived behavioral control and intentions were in line with our expectations, the significant effect of condition on behavior was surprising. As participants completed the TPB questionnaire directly after playing the serious game, they had no opportunity to change their actual behavior in line with their self-reported behavior. This suggests that other forces might have affected these results. Two alternative explanations come to mind. First, there is the potential of socially desirable responding. However, if this explanation holds true, we would expect the participants in the control game plus information condition to report higher levels of behavior compared with the control condition, which was not the case. The second explanation is that of consistency. As participants were asked about attitudes, subjective norms, perceived behavioral control, and intentions in the same questionnaire that also measured behavior, participants might have felt the urge to be consistent in their responses to the various questions, resulting in inflated self-reported behavior.

Limitations and future research

The first limitation of this study lies in the limited evidence for behavioral change as a result of playing the cybersecurity game that goes beyond the effects of the TPB predictors. Although it might be reasonable to assume that if all TPB predictors are positively influenced by the serious game, this will lead to some change in actual behavior, our study does not present convincing proof that that is the case. Our study found an effect of condition on self-reported behavior where this was not expected, and no objective behavioral measurement was included. The second limitation is that we did not investigate to what extent the reported changes lasted over time. In our study, the outcome measurement followed directly after completing the serious game, so it remains unclear how long the effects of serious games on TPB predictors last.

This study is the first to demonstrate the potential of serious games in influencing TPB factors in relation to cybersecurity. Although our results are promising, further research is needed. In a practical sense, future research should investigate the effects of serious cybersecurity games on objective behavioral measures, as well as measuring whether these effects last over time. In addition, this study consisted of an online serious game that could be played individually. As serious games are often designed for teams in offline settings, the potential added benefit of interacting with others should be examined. It might be that subjective norms are more effectively influenced in team settings than in our individualistic approach. Furthermore, this might strengthen the perceived behavioral control as team members can share best practices beyond solutions offered by the game. Similarly,

Table 3. Descriptive Statistics and Analysis of Variance Results

	Descriptive statistics			*ANOVA statistics*			
	Control game n = *89* M (SD)	*Control game plus information* n = *80* M (SD)	*Cybersecurity game* n = *89* M (SD)	F-*statistic*	$df_{between}$	df_{within}	p
Attitudes	16.61 (2.84)[a]	16.93 (3.17)[a]	18.01 (2.31)[b]	6.20	2	255	0.002
Subjective norms	12.25 (3.14)[a]	12.40 (3.39)[a,b]	13.53 (3.28)[b]	4.04	2	255	0.019
Perceived behavioral control	13.80 (3.59)[a]	14.00 (3.78)[a]	15.31 (2.95)[b]	5.02	2	255	0.007
Intention	14.55 (3.84)[a]	14.65 (4.36)[a]	17.08 (3.10)[b]	12.56	2	255	0.000
Behavior	14.75 (3.74)[a]	14.48 (4.63)[a]	16.37 (3.53)[b]	5.76	2	255	0.004

In each row, different superscript letters indicate significant differences between groups after correcting for multiple comparisons.
ANOVA, analysis of variance.

participants might be more attentive in an offline setting than when playing the game on their computer or mobile device. Offline team-focused serious games could, therefore, be even more effective, or result in longer-lasting changes in TPB predictors and behavior, compared with the individual online setting that was used in this study. We believe serious games are a promising approach to train and educate end-users in becoming more cybersecure, thereby better protecting themselves and the organizations they work for.

Authors' Contributions

J.D. conceived of the study and collected the data; T.v.S. and J.D. designed the study, conducted the analysis, drafted, and critically revised the article; T.v.S. supervised the project.

Author Disclosure Statement

T.v.S. has nothing to disclose. J.D. was employed by an organization that designs serious games at the time of conducting the research reported in this article.

Funding Information

No funding was obtained for the research reported in this article.

References

1. Ponemon Institute. (2018) *Cost of data breach study: impact of business continuity management*. IBM, https://www.ibm.com/downloads/cas/AEJYBPWA (accessed Jul. 9, 2020).
2. Saini H, Rao YS, Panda TC. Cyber-crimes and their impacts: a review. International Journal of Engineering Research and Applications 2012; 2:202–209.
3. van Steen T, Norris E, Atha K, et al. What (if any) behaviour change techniques do government-led cybersecurity awareness campaigns use? Journal of Cybersecurity 2020; 6:1–8.
4. Cheung RS, Cohen JP, Lo HZ, et al. (2011) Challenge based learning in cybersecurity education. WorldComp'11: The World Congress in Computer Science, Computer Engineering and Applied Computing, Las Vegas.
5. McDaniel L, Talvi E, Hay B. (2016) Capture the flag as cyber security introduction. In *Proceedings of the 2016 49th Hawaii International Conference on System Sciences (HICSS) (HICSS '16)*. USA: IEEE Computer Society, pp. 5479–5486.
6. Gondree M, Peterson ZNJ, Denning T. Security through play. IEEE Security and Privacy 2013; 11:64–67.
7. Michael D, Chen S. (2006) *Serious games: games that educate, train and inform*. Boston, MA: Thompson Course Technology PTR.
8. Charsky D. From edutainment to serious games: a change in the use of game characteristics. Games and Culture 2010; 5:177–198.
9. Sitzmann T. A meta-analytic examination of the instructional effectiveness of computer-based simulation games. Personnel Psychology 2011; 64:489–528.
10. Haggman A. Cyber wargaming: finding, designing, and playing wargames for cyber security education. PhD thesis, Royal Holloway University of London, 2019.
11. Martínez-Durá RJ, Arevalillo-Herráez M, García-Fernández I, et al. (2011) Serious games for health and safety training. In Ma M, Oikonomou A, Jain LC, eds. *Serious games and edutainment applications*. London: Springer-Verlag.
12. Hendrix M, Al-Sherbaz A, Bloom V. Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games 2016; 3:53–61.
13. Ajzen I. The theory of planned behavior. Organizational Behavior and Human Decision Processes 1991; 50:179–211.
14. Thomas R, Cahill J, Santilli L. Using an interactive computer game to increase skill and self-efficacy regarding safer sex negotiation: field test results. Health Education and Behavior 1997; 24:71–86.
15. Fellnhofer K. Game-based entrepreneurship education: impact on attitudes, behaviours and intentions. World Review of Entrepreneurship, Management and Sustainable Development 2018; 14:205–228.
16. Courbet D, Bernard F, Joule RV, et al. Small clicks, great effects: the immediate and delayed influence of websites containing serious games on behavior and attitude. International Journal of Advertising 2016; 35:949–969.
17. Fijnheer JDL, van Oostendorp H, Veltkamp RC. (2019) Enhancing energy conservation by a household energy game. In Gentile M, Allegra M, Söbke H, eds. *Games and learning alliance*. Cham: Springer International Publishing, pp. 257–266.
18. DeSmet A, Van Ryckeghem D, Compernolle S, et al. A meta-analysis of serious digital games for healthy lifestyle promotion. Preventive Medicine 2014; 69:95–107.
19. Berger J, Bawab N, De Mooij J, et al. An open randomized controlled study comparing an online text-based scenario and a serious game by Belgian and Swiss pharmacy students. Currents in Pharmacy Teaching and Learning 2018; 10:267–276.
20. Marne B, Wisdom J, Huynh-Kim-Bang B, et al. (2012) The six facets of serious game design: a methodology enhanced by our design pattern library. In Ravenscroft A, Lindstaedt S, Delgado Kloos C, et al., eds. *21st century learning for 21st century skills*. Berlin: Springer.
21. Le Compte A, Elizondo D, Watson T. (2015) A renewed approach to serious games for cyber security. In Maybaum M, Osula A.-M, Lindstrom L, eds. *7th International Conference on Cyber Conflict: Architectures in Cyberspace, (CYCON)*. Tallinn: NATO CCD COE Publications.
22. Mitsgutch K. (2011) Serious learning in serious games: learning in, through, and beyond serious games. In Ma M, Oikonomou A, Lain LC, eds. *Serious games and edutainment applications*. London: Springer.
23. Poulter DR, Chapman P, Bibby PA, et al. An application of the theory of planned behaviour to truck driving behaviour and compliance with regulations. Accident Analysis and Prevention 2008; e40:2058–2064.
24. McMillan B, Conner M. Using the theory of planned behaviour to understand alcohol and tobacco use in students. Psychology, Health and Medicine 2003; 8:317–328.

Address correspondence to:
Dr. Tommy van Steen
Institute of Security and Global Affairs
Leiden University
Turfmarkt 99 Room 4.03
The Hague 2511 DP
The Netherlands

E-mail: t.van.steen@fgga.leidenuniv.nl