Mapping of cybersecurity games onto CyBOK

Joseph Hallett and Benjamin Shreeve

February 15, 2022

Tabletop learning exercises—such as *Decisions & Disruptions (DD)*[1], *[dox3d!]*[2] and *Elevation of Privilege (EoP)*[3]—are used by organisations to help educate and train their workforce. What their employees learn from these games, and to what depth is often less clear. Cyber Security Body of Knowledge (CyBOK) has already been used to map curricular frameworks[4] and professional certifications, and better understand the benefits they provide. Unlike certifications, however, games cannot be mapped by analysing content alone as learning outcomes come about through play. Purely static mapping methods may not be appropriate to capture the knowledge gained from play.

To better understand what these games are teaching we mapped three cyber security games onto CyBOK v1.1[5], first by analysing the *contents of the games* and secondly by analysing *people playing the games* looking specifically for moments where players either used their own cyber security experience to influence how they played the games or where the games prompted the players to reflect on how the game play related to their own cyber security experience.

We find that whilst the games contain a broad range of cyber security content, the learning outcomes when playing the games suggest that what you get out of the game may differ.

Method

We used a mixed-method of analysis[6] in two distinct phases:

Phase 1: Analysis of game content Cards, assets and material associated with each game was listed and coded independently by two researchers using 23 apriori codes (each of the 21 CyBOK KA, as well as a code for the introduction, and a code to represent knowledge outside of the scope of CyBOK, see Appendix) as well as looking for emergent codes (in an analysis reminiscent of open coding[7]). To decide where in CyBOK any particular piece of content should be mapped a variety of resources were used including the CyBOK mapping reference[8] and the researchers own knowledge of the core CyBOK text[9]. Once the coding had been completed independently the two researchers discussed their mappings together to reach an agreed mapping for the content of each game.

Phase 2: Analysis of game play learning To assess the learning outcomes that emerged when playing the games we recorded participants playing the games and transcribed[10] their conversations. These transcriptions were coded to highlighted examples of where the participants related the game play to their own cyber

Acknowledgement. This work was supported by the Cyber Security Body of Knowledge (CyBOK) call for funded projects to develop resources around CyBOK v1.1.

[1] Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. The good, the bad and the ugly: A study of security decisions in a cyber-physical systems game. *IEEE Transactions of Software Engineering*, 45(5):521–536, 2019

[2] Mark A. Gondree and Zachary N. J. Peterson. Valuing security by getting [d0x3d!]: Experiences with a network security board game. In *6th Workshop on Cyber Security Experimentation and Test, CSET '13, Washington, D.C., USA, August 12, 2013*, 2013

[3] Adam Shostack. Elevation of privilege: Drawing developers into threat modeling. In *2014 USENIX Summit on Gaming, Games, and Gamification in Security Education, 3GSE '14, San Diego, CA, USA, August 18, 2014*, 2014

[4] Joseph Hallett, Robert Larson, and Awais Rashid. Mirror, mirror, on the wall: What are we teaching them all? Characterising the focus of cybersecurity curricular frameworks. In *2018 USENIX Workshop on Advances in Security Education, ASE 2018, Baltimore, MD, USA, August 13, 2018*, 2018

[5] Andrew Martin, Awais Rashid, Howard Chivers, George Danezis, Steve Schneider, and Emil Lupu. *The Cyber Security Body of Knowledge*. University of Bristol, 2021. Version 1.1

[6] Matthew B. Miles and A Michael Huberman. *Qualitative data analysis: an expanded sourcebook*. Sage, 1994

[7] Anselm Strauss and Juliet Corbin. Basics of qualitative research techniques. 1998

[8] Lata Nautiyal, James Clements, Joseph Hallett, Benjamin Shreeve, and Awais Rashid. CyBOK mapping reference. Issue 1.3

[9] Both researchers have worked extensively with CyBOK including in its production and existing mappings.

[10] Transcription was done through Microsoft's Office365 services.

security experience—either to influence how they played the game or to reflect on how game-play related to real-life—and then these reflections were mapped onto CyBOK.

Case Studies

All three games were played by two teams of players, with varying degrees of cyber security experience. The first session was played by a team of 6 players, and the second a team of 4. All games were overseen by an experienced *games master* who introduced the players to each of the games and guided them through the play. Summary statistics about each of the sessions is shown in Table 1.

	Decisions & Disruptions	[d0x3d!]	Elevation of privilege
Content			
Mapped	40/41	41/41	70/75
Session 1			
Players	6	6	6
Play time	29	48	22
Mapped	30/419	1/937	25/228
Session 2			
Players	4	4	4
Play time	31	76	12
Mapped	11/285	1/1144	5/60

Table 1: Statistics about play sessions with each of the games. Mapped expressed as a fraction of *things mapped / things possible* to map. Play times expressed in minutes.

Decisions & Disruptions

DD is a game about making cyber security investments for a hydro-electric plant. Players are given a choice of *mitigations* (including infrastructure, upgrades, training and audits—see Figure 3) to invest in and a finite budget per round. Over the course of four rounds they must chose which investments to deploy in their plant to protect their business. At the end of each round players are told about what attacks they suffered and which attacks they managed to defend against as well as any financial penalties they suffered. Our participants—some of whom had played the basic game before—played a variant of DD developed by the *London Metropolitan Police Service* to help raise awareness about cyber security risks to organisations and the importance of risk thinking, and to collect data about how people make risk decisions in teams[11]. This variant was novel to all players.

To map the contents of the game we included each of the mitigation cards as well as each of the different attack types players could suffer within the game and the different adversaries who could attack them (both taken from the DD *Game Master's Guide*). This produced 41 items which we mapped to CyBOK (Figure 1). The mapping of the content of the game shows a focus placed on *malware and attack technology* and *adversarial behaviours* coming from the various attackers and attacks that players can suffer alongside a number of other mappings, including references to CCTV that belongs to *physical security* and is outside of the scope of CyBOK.

When playing the game, however, we see the focus shift and discussion moves to being predominantly about topics within the *risk management and governance* Knowledge Area (KA) (Figure 2). For example, in the second session one player encouraged the team to invest in the *security training* because, based on their experience, that was the most likely first stage in an attack

> "...we need security training for people, because if someones sending them phishing emails, yeah, that's what happens usually first."

Another player used their experience of attacks in the real world

[11] Benjamin Shreeve, Joseph Hallett, Matthew Edwards, Pauline Anthonysamy, Sylvain Frey, and Awais Rashid. "So if Mr Blue Head here clicks the link..." Risk thinking in cyber security decision making. *ACM Trans. Priv. Secur.*, 24(1):5:1–5:29, 2020; and Benjamin Shreeve, Joseph Hallett, Matthew Edwards, Kopo M. Ramokapane, Richard Atkins, and Awais Rashid. The best laid plans or lack thereof: Security decision-making of different stakeholder groups. *CoRR*, abs/2104.00284, 2021

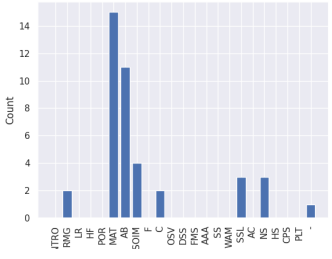


Figure 1: Mapping of the contents of DD onto CyBOK.

to argue for prioritising securing the back-end offices over the plant infrastructure itself:

> "So most of the attacks started from IT side, so we might secure that before really caring about this one. I mean, you cannot get here without compromising here."

Overall this paints a picture of DD as a game that contains a range of cyber security content but which promotes consideration of the *risk management and governance* aspects amongst its players and encourages them to reflect on their experience to decide how to play—exactly what the game was designed to promote.

[dox3d!]

[dox3d!] is a board game that aims to introduce students to network security terminology and cyber security basics. Players take on the roles of various hackers attempting to compromise a network of cards dealt out as a board. Players can compromise cards by flipping them over and move between compromised cards on the board. In each round players can work to complete their goals by playing cards in their hand, ultimately aiming to collect a number of items on the board, get to an escape card, and deploy a zero-day card.

When mapping the content of the game we mapped all the cards available to the players that could either be drawn from a deck or be part of the board. Whilst the mapping (Figure 6) appears to show a strong focus on *risk management and governance*, the mapping is skewed by the patch cards which are all mapped to that KA[12]. Overall the game contains a range of cyber security content and devices, broadly representing what you would expect to see in a corporate network.

In both sessions the teams of players we observed enjoyed playing [dox3d!] and opted to play the game twice in a row. However in terms of reflection on cyber security experience and relating it to the game we saw next to none—just one bit of conversation could be mapped in each session (Figure 5). In the first session a player remarked that the *patching* step of the game (where two flipped compromised squares of the board are *patched* at random returning them to an uncompromised state) was somewhat unrealistic:

> "But isn't it difficult for the team to actually patch things unless they are like spot on with what they're patching from?"

The only point of reflection in the second session was made by the Game Master. They noted that as the game was being played the players seemed to avoid the *firewall* square when choosing where to move; and joked that this was opposite to real life:

> "Good good good tactical move that. Firewall—don't care about that. True, but I love that that as hackers, the firewall is the only thing that consistently you're consistently not attacking. Being careful."

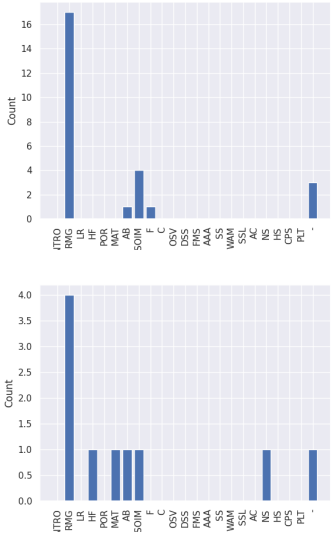


Figure 2: Mappings of players' reflections of their cyber security experience when playing DD onto CyBOK from two teams of players playing DD.

Figure 3: Example asset card from DD, representing an investment in staff training.

[12] Each turn a number of compromised parts of the board reset based on which patch cards are drawn. Patching infrastructure is part of the *risk management and governance* KA.

So what did they discuss if not cyber security? Mostly their possible moves in the game itself and tactics. Whilst they would discuss whether they could move from the *firewall* square to the *DNS server* the moves were not related back to any actual cyber security experience, or pivoting between systems in real life. As one player put it when discussing the game itself:

"Wait, this is luck?"

What does this mean for educators? Whilst [dox3d!] is a great game for introducing cyber security vocabulary and concepts we could see limited evidence that the game promoted cyber security reflective learning from play alone. The [dox3d!] website recommends using [dox3d!] as a starting point for discussing cyber security concepts in a classroom and provides curriculum modules to for parents and teachers. Whilst [dox3d!] is a great tool for getting people enthused about cyber security (all our participants enjoyed the game—the second session ran for over an hour playing the game) it did not appear to promote cyber security thought or reflection without supplemental prompting.

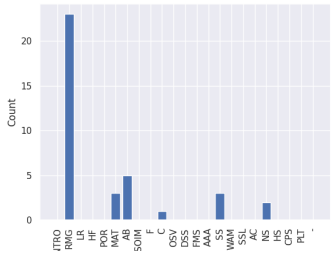


Figure 4: Mapping of the contents of [d0x3d!] onto CyBOK.

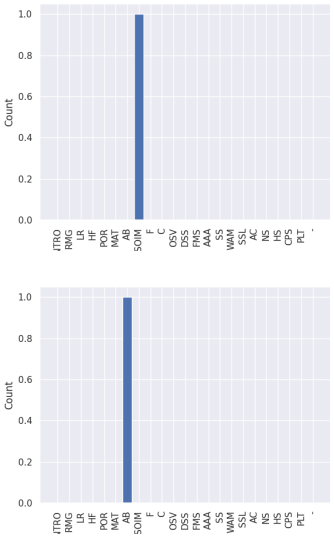


Figure 5: Mappings of players' reflections of their cyber security experience when playing [d0x3d!] onto CyBOK from two teams of players playing DD.

Elevation of Privilege

/shell Elevation of Privilege (EoP) is a threat modelling card game developed by Adam Shostack. Players start with a system to consider; are dealt cards from a deck with five suits based on STRIDE[13] and attempt to win tricks by playing cards in the style of whist. Each card has a prompt on it to consider a threat or risk. When playing the cards the player must describe how that threat applies to the system they are considering: if they cannot then they lose the trick.

To map the content of the game each of the 75 cards was mapped onto CyBOK (Figure 8). Whilst the game focuses on *software security* it covers various other aspects of cyber security and threat modelling. It also contains several *make up your own attack* cards that could not be mapped onto CyBOK as they were too vague to fall into any KA.

Figure 6: Example card taken from [d0x3d!]. [13] Spoofing, Tampering, Repudiation, Information Disclosure and Elevation of Privilege; see the *Secure Software Lifecycle* KA within CyBOK.

When playing EoP in our sessions our players were asked to consider a hypothetical bank as the system under consideration. The results from the mappings of the play during these sessions are shown in Figure 9 and show a focus on *software security*, *authentication, authorisation and accountability* and *network security*: all areas covered by the STRIDE threat modelling system EoP is based on.

When the first team played the game we saw the prompts from the cards encourage them to think about and reflect on different attacks to the system and often link it to their wider experience or other areas. For example one player realised that the system might include a weak permission group that was actually equivalent to anyone with a social media account:

"So an attacker can alter information in a data store because it has

> weak or open permissions or includes a group which is equivalent to anyone—parentheses: anyone with a Facebook account?"

In another example a player was prompted by one of the cards to share a story about a cyber security with a different system they once saw:

> "In banks they use a lot of sharing. . . sorry I am telling you *in banks* [. . .] there is a core banking solution the was built. . . "

In the second session we saw similar reflections made by the players: linking threats to risks and then working through how they could be used to compromise the whole system:

> "[. . .] and that can anonymously connect because we expect the authentication to be done at a higher level [. . .] 'cause if I get through the authentication I can just go through straight as somebody with, like, admin privileges."

Unfortunately, a lack of familiarity with the system they were examining in both sessions meant that the players tired of playing EoP quickly (Table 1). As the game master put it:

> "I can never work out how you want to play this without an enormous amount of cyber security knowledge. Yeah there are bits of this where I look at it and I go *'OK. I don't know how to apply that'*."

EoP encouraged players to consider cyber security and prompted reflection when the players were very familiar with the system they were thinking about. When the players were less familiar it lead to some confusion. Also: because of the random nature of the game, the reflections of the players varied depending on which cards they were dealt. In the second session players randomly got more cards about *spoofing* (which were predominantly mapped to *authentication, authorisation and accountability*) and so more of their discussion focused on these aspects. If they had played for longer, EoP may have prompted more diverse reflections.

Figure 7: A card from EoP: the *Jack of Spoofing*.

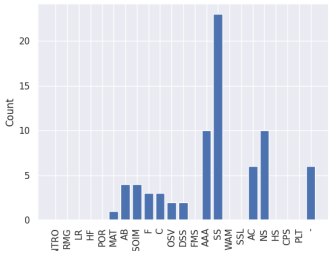
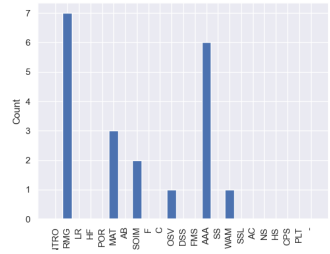


Figure 8: Mapping of the contents of EoP onto CyBOK.



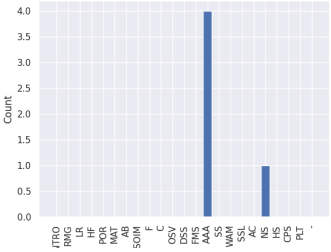


Figure 9: Mappings of players' reflections of their cyber security experience when playing DD onto CyBOK from two teams of players playing DD.

Lessons Learned

Mapping games onto CyBOK can help clarify the content and focus of different games, however the dynamic nature of games makes mapping more problematic than other mappings where the content is more static—such as curriculum frameworks, courses and textbooks. Having undertaken three of these mappings we would urge that should other researchers attempt more mappings in future, they consider the following points when mapping.

Consider how people interact with the materials. When mapping the content of DD and EoP we didn't see much content relating to *risk management and governance*, but when playing the games it did prompt discussion of aspects related to it. Similarly [dox3d!] contained a broad range of cyber security themes but they didn't

influence how people played the game and appeared to be essentially decorative. To properly understand the content of something you need to consider how people interact with it—else you'll miss content that comes interactively and may overvalue the benefit of content that does not influence people.

Randomness affects things. When playing EoP we found participants got different things out of the sessions as they drew different cards. We analysed the sessions from just two games of EoP and with different participants thinking about different things we would have almost certainly seen different things. With DD and [dox3d!] we saw more consistent results from playing the game—but DD does not include any randomness.

Not everything is about cyber security. When playing all the games most of what people talked about didn't relate to cyber security. On average just 5% of the time people spent talking they were reflecting on cyber security (Table 1). This is skewed somewhat by [dox3d!] where there was almost no cyber security discussion, but still is in general true. The other discussion when playing a game is also interesting however, and future mappings should explore this further. In particular meta-discussion about the games themselves may be interesting as it captures how people perceive the game unfolding and this may impact how they perceive cyber security events unfolding: if games have taught them that the events are random then when seeing a real cyber security event perhaps they may also think that these events are largely random?

There isn't a lot to map. Whilst the games did contain a reasonable amount of cyber security content, there was relatively little reflection we could identify in the players discussion whilst playing the games. Consequently traditional agreement metrics such as *Cohen's* κ are of limited use owing to the low level of cyber security related codes identified within lengthy exchanges. Even when mapping the games' content themselves, agreement between the two coders was relatively low (fair–moderate agreement).

Conclusions

We have presented the mappings of three games about cyber security: DD, [dox3d!] and EoP. We find that whilst these games contain a broad (and different) range of cyber security content the reflection they promote can differ from the source material. Further work is needed to establish proper mapping techniques to better understand the content of these games in terms of CyBOK as current mapping approaches fail to account for what people learn whilst playing. Future work may benefit from a between subjects style research method, working with participants with no cyber security

experience in order to understand the learning effects of these exercises. However, establishing the difference between awareness of terms and actual understanding remains a challenge.

Appendix: Codebook

When mapping on to CyBOK the following apriori codes were used to capture the relationship with CyBOK:

Intro CyBOK introduction.

RMG Risk management and governance.

LR Law and regulation.

HF Human factors.

POR Privacy and online rights.

MAT Malware and attack technologies.

AB Adversarial behaviour.

SOIM Security operations and incident management.

F Forensics.

C Cryptography.

OSV Operating systems and virtualisation.

DSS Distributed systems security.

FMS Formal methods for security.

AAA Authentication, authorisation and accountability.

SS Software security.

WAM Web and mobile security.

SSL Secure software lifecycle.

AC Applied cryptography.

NS Network security.

HS Hardware security.

CPS Cyber-physical systems security.

PLT Physical-layer and telecommunications security.

- Out of the scope of CyBOK.

When analysing transcripts for cyber security reflections the following codes were used:

Reflection Indicates some reflection by a player on a cyber security theme.

⋆*Meta* (Emergent code.) Indicates reflection on the game and it's mechanism by players.

Appendix: Datapack content

Alongside this report we also offer the data collected and the mappings done as a datapack. The contents of this datapack are as follows:

Application/ The grant application for this small grant.

Ethics/ The ethics agreements in place for this project, including consent forms.

Figures/ Generated mapping charts and figures used in this report.

GNUmakefile Script to run all analysis and produce all charts.

Mappings/ Raw mappings data from each of the games content and for each of the sessions.

report.bib Bibliography for this report.

report.tex Source code of this report.

Resources/ Content analysed for each of the games.

Scripts/ Scripts used to analyse the mappings.