Imagining and Anticipating Cyber Futures with Games

Andreas Haggman[1]
Head of Cyber Advocacy
UK government department

Abstract: This short chapter considers the relationship between games and futures, with specific focus on cyber security. Games and gamification have received renewed attention in both academia and industry over the past ten years. Within this broad field, the genre of wargaming occupies a significant but often underappreciated space.

Unlike what some observers might argue, wargaming is not just an activity for history anoraks with an overly keen interest in the past. Wargaming can indeed be used to better understand historical events, but it can also be used to explore the dynamics of the present or employed as a highly imperfect crystal ball to gaze into the future. When done right, wargaming can be a powerful tool to engage audiences with little subject matter expertise or game playing experience.

Three core arguments are made in this chapter. First, wargames can provide structure for players to imagine futures. Second, wargames can prepare players for the future by enabling them to anticipate emotions. Lastly, cyber wargames should avoid the trap of becoming enamoured with the technology of cyber security.

The chapter is grounded in diverse literature, drawing on material from cultural studies, strategic studies, modelling and simulation and history. Readers will find theoretical insights into the uses of games alongside practical advice for those seeking to use wargames in a cyber security context.

Keywords: *Cyber, multi-domain, cross-domain, concepts, Russia, China*

[1] Disclaimer: This work represents the personal opinions of the author. This work does not represent the opinion of the UK government and nothing in this document should be construed as UK government policy nor UK government endorsement of the work.

1. INTRODUCTION

Beyond frivolous entertainment, games have practical uses that are often overlooked. Wargaming is a genre of games and gamification that focuses on scenarios involving conflict. Conflict is not limited to direct military confrontation—a primary area of interest for NATO—but can encompass any situation where competition or strife is prevalent.

In cyberspace, current conflict is best characterised as ongoing competition below the level of military confrontation. State actors are continually jostling for position on adversaries' networks, seeking to maintain a foothold without causing undue disruption. Meanwhile, non-state hostile actors, such as organised crime groups, are running campaigns targeting private companies for financial gain.

For many people, cyber wargames conjure a vision of large-scale capture-the-flag events where teams of technical experts attempt to attack and defend their computer networks. Such exercises mimic the conflict we see in cyberspace, but in focusing on technology and tactics, the political and strategic dimensions of cyber security and cyber conflict are often missed. Participants learn how to defend against an attack, but they are not challenged to ask why an attack might occur in the first place.

In the cyber domain, NATO has been an active proponent of exercises, including Locked Shields and Crossed Swords. While both events focus on the technical side of cyber security—the former on strategic decision-making and the latter on operational aspects—these exercises have developed over time to include non-technical elements like legal and public relations. This suggests that the culture in NATO is amenable to using types of games outside the classic conception of a cyber wargame.

Wargames that remove the technical barrier allow participants from a broader range of backgrounds to contribute insight. Even deceptively simple wargames can be effective at prompting participants to imagine and convey futures in a focused way. By sharing these conceptions with other participants, wargaming sessions can result in a joined-up appreciation of future threats. Wargaming, most simply defined, is a 'model or simulation [...] whose sequence of events affects and is, in turn, affected by players representing the opposing sides' (Curry, 2011: p. 157). In this seminar definition, Peter Perla originally referred explicitly to warfare, but the concept can be extended to almost any instance of conflict, both inside and outside military domains. Whatever the activity portrayed, whether it is manoeuvring armoured vehicles or making a business investment decision, wargaming is ultimately focused on the human participants and their actions and experiences.

Throughout this chapter, the author seeks to promote the idea that in cyber security, a simple wargame can go a long way. Tabletop exercises are perhaps the ultimate in simplicity, but often fail to go beyond superficial what-if scenarios and can deteriorate into unproductive ‘Bunch of Gals/Guys Sitting Around a Table’ (BOGSATs). Wargaming as a method is replete with tools and techniques that are effective at creating realistic scenarios and generate a high level of player engagement. Matrix games, for example, are types of wargames that bring structure and competition to tabletop exercises through the use of expert adjudication (akin to a professional ‘Dungeon Master’) and a modicum of gaming paraphernalia such as dice or cards. The author’s own experience with a cyber strategy wargame is outlined in Section Five.

This chapter explores one particular dimension of wargaming: how it engages the forward-looking faculties of participants, specifically focusing on imagination and anticipation. In Section Two, the links between games and imagination are explored, with close reference to effective methods for enabling players to imagine futures at a political or strategic level. Section Three extends this discussion to anticipation and how games can emotionally prepare players for the future. Section Four considers the uncertain future of cyber capabilities, before section Five concludes with some actionable takeaways for the reader.

2. Futures and Imagination

The further we seek to gaze into the future, the more we have to employ our imaginative rather than our analytical faculties because of the increased uncertainty. Just consider science fiction literature, which often seems to become more far-fetched the further into the future it is set. At the same time, futures imagined on a shorter time frame can often be realistic; consider the apparent prescience of some of the works from authors like H. G. Wells (1908).

When we play games, we exercise our ability to imagine the future because we need to imagine the context in which future game actions will take place. After studying competitive chess players, Gary Fine (2014) concluded that players’ strategy, consisting of a series of planned moves—or ‘the line’—is the core mechanic in that game, not the moves themselves (p. 323). These ‘lines’ require an ability to anticipate the opponent’s strategy to construct the imagined game future.

Chess, however, is a highly abstract game and teaches us little about contemporary strategy or politics. In his later life, political theorist Guy Debord attempted to amalgamate the imaginative capacities of wargaming with his leftist political ideals. His Game of War set out to capture the struggle between a bleak ‘historical present’ and an unattainable future of ‘utopian imagination’ (Galloway, 2009: pp. 151-152). Ultimately, Debord became obsessed with ‘the sublimation of antagonistic desire into an abstract rulebook’ and Game of War ended up as something which looked more like chess with some added mechanics around military logistics than a game of political strife (Galloway, 2009: p. 28).

Perhaps Debord, and others seeking to invoke imagined futures, can learn from Pericles of ancient Athens. Pericles was a master orator, able to convincingly convey potential futures to spur Athenians to action. What made Periclean futures so potent was their grounding in reality. According to Lawrence Freedman (2013), Pericles drew 'from an existing reality but moved beyond it' and the plausibility of a future was 'derived from its practicability' (p. 49). As an example, in cyber security, a future where only friendly actors derive the benefits from a technology like quantum computing seems more Debordian than Periclean. Instead, an imagined future involving quantum computing must consider the viability of this technology also being in the hands of hostile actors.

When designing wargames, the key to success is to understand the purpose of the game and the future it is intended to explore. A tactical awareness training tool might lend itself to a chess-like design where players can imagine 'lines' such as hopping from node to node while penetrating a network. Conversely, a strategic game exploring international political dimensions may need less of a strict rule set and instead provide realistic foundations for players to extrapolate their own imagined futures.

3. Futures and Anticipation

As an extension of imagining futures, anticipation has been described by Vincanne Adams et al. (2009) as 'an epistemic orientation towards the future' (p. 254). In other words, anticipating futures involves creating knowledge about the future, thereby negating surprise. In everyday usage, 'surprise' can be used either positively or negatively—compare a surprise birthday party to a surprise conference paper rejection. Wargaming is often concerned with negating negative surprises. David Hulse et al. (2016) identify that a core use of modelling (closely allied to wargaming) is understanding 'when, where and how "reducible ignorance" can be most effectually reduced vis-a-vis anticipated surprises' (p. 41). As tools for anticipating futures, wargames enable knowledge creation which can help reduce surprise.

An important aspect of anticipation is the emotion contained within surprises. A birthday party is a pleasant surprise, while a paper rejection is unpleasant. When it comes to drivers of human behaviour, Roy Baumeister et al. (2007) attest that 'anticipation of emotion is more important than the actual emotion' (p. 174). While writing a paper, an author might contemplate the hurt associated with rejection and be compelled to make a greater effort to write a brilliant paper.

Because of its ludic nature, wargaming is closely associated with competition and personal performance. Wargames usually have winners and losers; the winners experience joy, elation and satisfaction, the losers are disappointed, angry and dissatisfied. One of the insidious features of wargaming is that players' in-game behaviour can be driven by anticipation of these emotions, rather than reasoned actions. However, the other side of this coin is that players become better prepared for the future by anticipating and eventually experiencing these emotions in the safety of the game environment. Wargames can help desensitise players to the extremes of emotions contained within surprises—or, indeed, other adverse experiences such as frustration, confusion, information deficiency or excess—so that when they encounter similar surprises and emotions in real life, the effects on their behaviour are not as drastic.

4. Cyber Futures

As domains of warfare have increased from two (land and sea), to three (air), to four (cyberspace) and five (space) (NATO, 2020), wargaming has been increasingly challenged to tackle the technological developments of the day. Sharon Ghamari-Tabrizi (2000) writes that during the Cold War, 'the technical horizon within which future wars would be fought would change constantly, albeit uncertainly' (p. 164). In the Cold War context, nuclear weapons dominated wargaming scenarios, yet the 'technical horizon' did not fluctuate as wildly as game designers of the time might have envisaged. With the benefit of hindsight, we can say that nuclear weapons of greater yields could be delivered further and faster in the 1980s than the 1950s, but the overall nature of these weapons did not change, and indeed remains the same today.

With cyber capabilities, wargaming finds itself looking at another technical horizon. The past 15 years have only provided glimpses of what cyber operations might look like at full scale—Estonia in 2007, Stuxnet in 2010 and NotPetya in 2017 are excellent examples. It is possible to imagine a future where cities go dark as power plants are shut down at the whim of an adversary. Indeed, such doom-mongering has been successful at capturing public and political attention—not dissimilar from the scenarios of the Cold War.

However, perhaps these examples are more than glimpses—do these totemic operations represent the zenith of cyber capabilities? It is possible to imagine a future not unlike today where cyber capabilities are used sparingly because of their expense and their limited and unpredictable effects.

Or perhaps both of these imagined futures are incorrect and cyber capabilities have yet to reveal their final form. In the early 20th century, reams of strategic thinking were expounded on the novel concept of airpower and yet the technology that prompted this thinking was airships, not aeroplanes—recall that the Wright Flyer first took off in 1903, and that Giulio Douhet's seminal The Command of the Air was not published until 1921. Strategic thinking around cyber has similarly boomed in the early 21st century, but cyber capabilities of the future may make Stuxnet look like an inflatable blimp by comparison. The point here is that it is difficult to know when, or even if, technology will outpace strategic thinking.

5. Cyber Wargaming

When imagining and anticipating cyber futures, the lesson for wargaming is similar as for Wells' science fiction, Wells himself being an avid wargamer. In The War in the Air, Wells' characterisation of airpower was not wholly incorrect, though it was exaggerated because the technology in the novel was swiftly superseded. In cyber wargames, the technical aspects of cyber capabilities should be deemphasised and potential effects should be based on current observable reality rather than unsubstantiated hype.

That is not to say that cyber wargames should ignore technology. After all, cyber is a technical domain, not a natural one. But cyber wargames at the strategic level should not get bogged down in the relative merits of, say, ElGamal versus RSA encryption algorithms. Instead, the effect 'data is encrypted' would reasonably be the level of detail required for strategy games. By focusing away from the micro-level details of technology, participants in wargames can explore the macro-level strategic and political reasons why a cyber attack might occur and how to respond to it, without being burdened with the tactical minutiae of cyber security. These minutiae have their place in attack-defence exercises and capture-the-flag events, but these types of games do not readily lend themselves to the imaginative and anticipatory dimensions of wargaming.

From his experience of the 2010 Schriever Wargame organised by the US Air Force, George Foresman, former Undersecretary at the US Department of Homeland Security, stated that 'the lessons identified [...] are not futuristic concepts' (2010: p. 8). This sentiment seems to intimate a sweet spot for wargames to hit: create a scenario that participants can imagine as a plausible future and from which they can anticipate and learn lessons; but avoid a scenario that is overly 'futuristic' and which participants relegate to the realms of science fiction.

For those seeking to use wargames and who want to hit that sweet spot while avoiding the trappings of technology, a good starting point would be to keep it simple. A game does not necessarily need intricate graphics and advanced gameplay mechanics to be effective. For example, sample games found in Dark Guest (Curry & Rice, 2013) or The Handbook of Cyber Wargames (Curry & Drage, 2020) require only basic gaming paraphernalia – in many cases just a die. The real value comes from the players rather than the games themselves.

In the author's own experience, a cyber strategy wargame with a moderate degree of gaming paraphernalia has been successful at eliciting learning moments for players (Haggman, 2019). The game in question was loosely based on the UK National Cyber Security Strategy (HM Government, 2016) and used a game board, cards, dice, player characters and a set of rules to convey some limited detail about cyber security topics and dynamics. This was less simple than a matrix game but provided very direct discussion opportunities because players could assess the game components. Asking players what they would add to the game was often revealing in terms of what they understood to be important in cyber security, at both strategic and operational levels. Moreover, because the game was relatively easy to learn and purposely designed to be fun, it was highly engaging for players. Overcomplication can discourage player engagement. Simplicity incites imagination and anticipation, thereby realising the benefits associated with wargaming futures.

6. REFERENCES

Adams, V., Murphy, M. & Clarke, A. E. (2009) Anticipation: Technoscience, life, affect, temporality. *Subjectivity*. 8, 246-265.

Baumeister, R. F., Vohs, K. D., DeWall, C. N. & Zhang, L. (2007) How Emotion Shapes Behavior: Feedback, Anticipation, and Reflection, Rather Than Direct Causation. *Personality and Social Psychology Review*. 11 (2), 167-203.

Curry, J. (2011) *Peter Perla's The Art of Wargaming: A Guide for Professionals and Hobbyists*. The History of Wargaming Project.

Curry, J. & Price, T. (2013) *Dark Guest: Training Games for Cyber Warfare Volume 1 –Wargaming Internet Based Attacks*, 2nd ed.

Curry, J. & Drage, N. (2020) *The Handbook of Cyber Wargames: Wargaming the 21st Century*. The History of Wargaming Project.

Douhet, G. (1921) *The Command of the Air*. trans. Ferrari, D. Air University Press.

Fine, G. A. (2014) Strategy and Sociability - The Mind, the Body, and the Soul of Chess. *American Journal of Play*. 6 (3), 321-344.

Foresman, Hon. G. W. (2010) The Complexities of American National Security: Enabling A New Generation of Leadership. *High Frontier - The Journal for Space and Cyberspace Professionals*. 7 (1), 5-8.

Freedman, L. (2013) *Strategy: A History*. Oxford University Press.

Galloway, A. R. (2009) Debord's Nostalgic Algorithm. *Culture Machine*. 10, 131-156.

Ghamari-Tabrizi, S. (2000) Simulating the Unthinkable: Gaming Future War in the 1950s and 1960s. *Social Studies of Science*. 30 (2), 163- 223.

Haggman, A. (2019) 'Cyber Wargaming: Finding, Designing and Playing Wargames for Cyber Security Education'. PhD thesis, Royal Holloway University of London.

HM Government. (2016) 'National Cyber Security Strategy 2016-2021'. Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf. [Accessed 23rd October 2020].

Hulse, D., Branscomb, A., Enright, C., Johnson, B., Evers, C., Bolte, J. & Ager, A. (2016) Anticipating surprise: Using agent-based alternative futures simulation modeling to identify and map surprising fires in the Willamette Valley, Oregon USA. *Landscape and Urban Planning*. 156, 26-43.

NATO. (2020) 'NATO's approach to space'. Available at https://www.nato.int/cps/en/natohq/ topics_175419.htm. [Accessed 23rd October 2020].

Wells, H. G. (1908) *The War in the Air*. Available at: http://www.gutenberg.org/ebooks/780. [Accessed 23rd October 2020].