Cheating the Network: How Gamers Play the Infrastructure

Sean Willett & Mél Hogan
University of Calgary

ABSTRACT

Background *This article looks at how video game players interact directly with the infrastructure and networks that support digital games. To win, players are no longer simply "cheating the game," as with traditional behaviour considered deceptive or outside of the established rules, but are instead "cheating the network."*

Analysis *This distinction between these two types of cheating is important, and should be considered separate types of player interaction. "Cheating the network" is a new type of public engagement with network technology—one that runs counter to conventional views of a transparent, invisible media infrastructure.*

Conclusion and implications *By examining "cheating the network" separately from traditional forms of cheating in digital games, it is possible to reframe these player/game interactions as player/infrastructure interactions and view them through a critical lens of materiality.*

Keywords *Computer science; Electronic culture; Media/mass media; Cable systems; New media*

RÉSUMÉ

Contexte *Cet article examine comment les joueurs de jeux vidéo interagissent directement avec l'infrastructure et les réseaux dont dépendent les jeux numériques. En effet, pour gagner, les joueurs ne sont plus simplement en train de « tricher au jeu », adoptant un comportement trompeur ou hors normes traditionnel; ils sont plutôt en train de « tricher au réseau ».*

Analyse *Cette distinction entre deux façons de tricher est importante, car elle s'applique à deux types distincts d'interaction entre joueurs. « Tricher au réseau » est un nouveau type d'engagement public auprès des technologies du réseau—un engagement qui va à l'encontre de l'idée d'une infrastructure médiatique transparente et invisible.*

Conclusion et implications *En distinguant l'idée de « tricher au réseau » par rapport aux formes traditionnelles de tricherie aux jeux numériques, il est possible de recadrer les interactions entre joueur et jeu comme des interactions entre joueur et infrastructure et de porter un œil critique sur la matérialité de ces dernières.*

Sean Willett is completing an MA at the University of Calgary. He is a research assistant for Mél Hogan, producing a podcast on data centres. Email: srwillet@ucalgary.ca . **Mél Hogan** is an Assistant Professor (Environmental Media) at the University of Calgary. Her work focuses on data storage and genomic media. Email: mhogan@ucalgary.ca .

Canadian Journal of Communication Vol 44 (2019) 439–453 ©2019 Canadian Journal of Communication Corporation http://doi.org/10.22230/cjc.2019v43n3a3382

Mots clés *Informatique; Culture électronique; Médias/médias de masse; Systèmes de câbles; Nouveaux médias*

Introduction

Near the end of 2014, players of Bungie's multiplayer online game *Destiny* discovered that they could kill a god by pulling out their ethernet cables. "Thanks to some Bungie net-code flaws, you can easily beat Crota, the toughest boss in the game, by making one of your team members pull out their LAN cable," reported *Kotaku*'s Jason Schreier (2015, par. 2) in an article published a few weeks after a video demonstrating the method was posted on YouTube. To replicate the method, the players had to identify their team's "host," wait until a specific moment in the encounter, and then have their host intentionally sever their internet connection to their teammates—either by physically removing their ethernet cable or by force quitting the game. Teams of players were able to use this method to lock a powerful computer-controlled enemy in a state of permanent vulnerability by transforming a difficult, demanding encounter into a relatively simple one. "Is this cheating?" Schreier (2015, par. 13) asked at the end of his article. His answer: "absolutely."

This was not the first time that *Destiny* players found an unconventional way to play the game. Soon after the game's launch, a technique was discovered that allowed players to trick another boss, Atheon, into falling off a platform to its death (Liebl, 2014). Similar to the cable-pulling strategy used on Crota, this method of beating Atheon made a difficult encounter much easier; both Bungie and *Destiny* players labelled it as an "exploit." Both methods were widely considered forms of cheating from within the gaming community, and Bungie quickly patched both tactics out of the game. However, there is a key difference between the two: with Crota, players were manipulating the game's physical infrastructure, not the game itself. While the Atheon exploit saw players take advantage of a character's artificial intelligence, the Crota exploit required players to take advantage of the very network that allows *Destiny* to operate. To freeze Crota into a kneeling position, players had to trick the game's underlying architecture by taking action outside of the virtual world of the game.

This type of intervention, in which players directly interact with the networks that support digital games, sits at a crossroads between critical media infrastructure studies (Bowker, Baker, Millerand, & Rives, 2010; Dourish, 2015; Hu, 2015; Mosco, 2014; Parks & Starosielski, 2015) and digital games studies (Conaway, 2017; Consalvo, 2007; Taylor, 2009). This article's contribution to these fields is in putting forward that players are no longer simply "cheating the game" but are instead "cheating the network." This distinction is important. In a practical sense, defining this distinction allows both scholars and game designers to better understand the ways in which players are interacting with network technology, identifying instances in which players attempt to interface with physical and digital infrastructure in an effort to manipulate an in-game world. The concept of "cheating the network" also enriches theoretical approaches to digital games, allowing scholars to reframe these player-game interactions as player-infrastructure interactions and view these interventions through a critical lens of materiality. This lens reveals the relationships between the different structures that comprise a game's infrastructure environment, and allows for an interrogation of the economic, political, and social drivers behind their formation. Additionally, "cheating the network" is not only a distinct type of cheating but also an atypical example of public engagement with network technology—one that runs counter to conventional views of a transparent, invisible media infrastructure (Parks & Starosielski, 2015). By examining "cheating the network" separately from traditional forms of cheating in digital games, we can begin to understand the context that has allowed this new conceptualization of infrastructure to emerge, and perhaps seek to replicate this awareness in other forms of infrastructure.

In order to begin exploring the idea of "cheating the network," this article first describes the structures used to support online digital game networks and argues that these are a form of media infrastructure. These infrastructures are positioned in relation to existing media infrastructure scholarship, and the unusual relationship between digital game players and online game networks is contrasted against typical understandings of public conceptions of infrastructure. This foundation will be used to examine the ways players take advantage of online game infrastructure, and how this behaviour differs from traditional forms of cheating in digital games. The article concludes with a definition of what constitutes "cheating the network," and how this term can be used to apply a media infrastructure studies approach to the analysis of player-game interaction.

Cables and code

In order to connect players to one another in a virtual world, online digital games rely on a vast array of invisible underlying structures (Armitage, Claypool, & Branch, 2006). Some of these structures are shared by other forms of digital media distributed over the internet, such as underground cable networks, broadband wiring in residential buildings, and personal Wi-Fi routers. Other support structures are used only by video games but are analogous to systems used by other media. These include publisher-owned servers used to ensure consistent world states among players, which function similarly to servers used to host websites or other online services (Armitage et al., 2006). Online games also use distinct application-level network protocols—rule sets that determine how connections are made between users and servers and how data packets are transferred between them—that need to properly communicate with other protocol layers (Andrés, López, José, Parra, & Torres, 2016).

While network protocols are not material in the same sense as the other structures mentioned, they are still vital components of the networks that connect online games. Other software-level structures are programmed into digital games for this purpose. Since many online games can only function as intended if all players share a game state that is consistent with other players' game states, the structural architectures of the software of these games are designed to hide the limits of physical networks. Memory management mechanisms that limit the amount of information sent between players—such as "zoning," where large game areas are invisibly separated into smaller, easier-to-load zones—are used to decrease latency caused by slow network transmission speeds. Latency that cannot be completely eliminated is often hidden from players using other, more complex invisible systems. In some games, especially those that require fast reactions, algorithms are used to predict player inputs milliseconds before they are actually entered, in order to better create an illusion of perfect simultaneity (Yahyavi & Kemme, 2013).

All of these structures, both physical and digital, comprise the media infrastructure environment that supports online games. As defined by Lisa Parks and Nicole Starosielski (2015), media infrastructures are "situated sociotechnical systems that are designed and configured to support the distribution of online signal traffic" (p. 4). This includes "hard" material structures—physical objects such as cables, satellites, and data centres—along with "soft" material structures such as network protocols. As Paul Dourish (2015) further argues, these protocols should be seen "as things that are designed to serve applications, to run on computational platforms, and to control infrastructures, bound up with and contributing to the material realization of them all" (p. 185). While they may not be material in the traditional sense, protocols shape and are shaped by the materialities of the networks they travel over and are just as integral to the operation of these networks as their physical components.

Code-level architectural mechanisms designed to allow games to function over these networks should also be considered examples of media infrastructure for similar reasons. In pushing for an "information infrastructure studies" approach to studying knowledge work (work that handles information for problem-solving purposes), Geoffrey C. Bowker and colleagues (2010) argue that conceptualizations of infrastructure should go beyond the idea of "tubes and wires" and include "the technologies and organizations which enable knowledge work" (p. 98). This same approach can be applied to the media infrastructure of online digital games: not only do they need the physical "tubes and wires" to connect players together, they also need the nonphysical architectures that allow online games to effectively use these material networks. Without software-level infrastructure such as the predictive algorithms mentioned above, or server-side time-manipulation techniques used to ensure players with varying latencies receive information at the same time (Armitage et al., 2006), designers of online games would not be able to create the illusion of simultaneity in their shared virtual worlds. Without that illusion, most popular online games could not exist in their current form.

Recognizing the essential nature of these infrastructures in the proliferation and operation of digital media is the basis of the emerging subfield of critical media infrastructure studies, a theoretical approach described by Parks (2015) as an effort to "account not only for the bodies of actors that appear on screen, but for those involved in supporting acts such as the trafficking of content, the flow of electrical currents, and the policing of audiovisual signals" (p. 356). This infrastructural view of media can push communications scholars to place more importance on the processes of distribution, the material nature of digital media, and the consequences of technological literacy (Parks & Starosielski, 2015). Works in critical media infrastructure studies have attempted to explore these questions in a number of different contexts: Starosielski (2015) analyzes how transoceanic cable networks have reinforced global power structures, Vincent Mosco (2014) explores how the metaphor of the cloud is used to obscure the negative impacts of data centres, and Tung-Hui Hu's (2015) frames big data as a direct continuation of older methods of enforcing political power.

To date, a critical media infrastructure approach has yet to be meaningfully extended into the realm of digital games. There is one notable exception: Evan Conaway's (2017) work extends theories of play into the realm of server architecture, but otherwise this topic remains largely underexplored. This article takes the first steps toward filling this gap in the literature, pointing to distinct aspects of online game networks that warrant a more detailed analysis. The most significant of these is the way online game players interact with online game infrastructure: instead of taking the network for granted, players actively engage with it, both inside and outside of the game.

The invisible made visible

As with other types of infrastructure, online game networks are not designed to be seen. As described by Susan Leigh Star and Karen Ruhleder (1996), infrastructure has an inherently transparent element, "in the sense that it does not have to be reinvented each time or assembled for each task, but invisibly supports those tasks" (p. 113). Infrastructures are specifically designed to blend into the background when operated correctly, allowing for people to use them repeatedly without the need to relearn or rebuild the system in every instance. Accordingly, infrastructures tend to only be noticed when they start to break down.

In addition to this inherent transparency, modern media infrastructures in particular are further made invisible by the higher degree of technological literacy required to understand how complex transmission systems function. This degree of technical literacy is far from universal. As described by Parks and Starosielski (2015), "public access to technical knowledge about infrastructures isn't equal; rather it is guided and constrained by social hierarchies of gender, race/ethnicity, class, generation, and nation" (p. 6). Socioeconomic divides have created a knowledge gap regarding infrastructure, further reinforcing the invisibility of the systems that control and distribute media. The language used to describe these systems also distorts public conceptions of media infrastructure. The metaphor of "the cloud," for example, evokes images of an immaterial, decentralized system, instead of the physical, hyper-centralized data centres the term actually represents (Levin & Jeffery, 2016). A consequence of this infrastructural transparency, whether intentional or not on the part of network engineers, is that the public tends to largely ignore issues surrounding media infrastructure. However, this is not the case with digital games. Issues surrounding online game infrastructure often garner a significant amount of attention, specifically from the people who play these games. For example, Ubisoft's decision to use a peer-to-peer (P2P) network architecture for its 2016 game *For Honor* resulted in over one thousand people signing a petition demanding the publisher switch to a dedicated server system (ipetitions, 2017). Far from infrastructure being invisible, players explicitly blamed *For Honor*'s pervasive lag issues on the type of infrastructure used to support the game, and they were able to collectively voice their opinion that a different system be used instead.

The ability to identify and articulate these concerns, along with the casual use of terms such as "dedicated server" and "peer-to-peer," seems to point to the digital games community as having some understanding of how these infrastructures work and, more interestingly, an understanding of the impact these infrastructures have on games. This is also not an isolated incident; the use of P2P networks in particular has become a recurring issue in the digital games community, with multiple developers facing backlash for using this type of architecture.

Why, then, do gamers have this knowledge? And how have they come to obtain it? This infrastructural literacy might be driven by infrastructural failure. In the case of *For Honour*, infrastructural failure resulted in widespread cases of players appearing to teleport from place to place, taking damage from invisible enemies, and being disconnected from matches at random. Players easily notice these intrusions into the game world, called "breaks in presence" by Jaeyong Chung and Henry J. Gardner (2012, pp. 1–2), due to the way they shatter the illusion presented by the game.

These errors can also break the "fairness" of a competitive game. *For Honor* players with bad connections and higher latency would move more erratically due to the game's lack of latency management infrastructure, therefore, they were more difficult for other players to hit (Alexandria, 2017). Infrastructural flaws such as these can undermine the competitive nature of a game, adding unpredictable variables that can cause widespread frustration in players. *For Honour*'s network issues were perceived as especially egregious due to Ubisoft marketing the game as an "esport," meaning that the game was intended for high-level competitive play (Newell, 2017).

When these errors do occur, designers often choose to communicate them to players using language that references infrastructure. Examples of these in-game messages include *lost connection to host*, *could not reach server*, or *network lag detected*, all of which explicitly link negative gameplay experiences with failures in infrastructure. For players who feel as though the illusion of the game world has been broken or that the fairness of the game has been compromised, there is a clear culprit to blame.

All of these factors have meant that, as opposed to the transparent nature of most media infrastructures, the networks of online games are constantly in the spotlight—both inside and outside of the world of the games themselves. With that in mind, the seemingly widespread technical literacy surrounding infrastructural issues possessed by the digital games community seems less a surprising aberration, and more a logical outcome of the nature of online games as a medium. But players of these online games have taken this understanding one step further. They have not only started to recognize the invisible infrastructures that support their games, they have also begun to use these infrastructures to their advantage.

Cheating the network

When designing network architecture for online games, engineers have to consider a number of interrelated factors and limitations set by both physical infrastructure and software. How much lag can be tolerated before players begin to notice? How much information can be sent over the network at once before that amount of lag is reached? What information must always be sent, and what information can be lost? The answers to these questions differ depending on the type of game the architecture needs to support, and the nature of the experience the game is attempting to create. Slower-paced games, for example, are less affected by high latency and use slower, more secure network protocols with less risk for data loss. This is in contrast to faster-paced games, which have tighter latency limits and often need to be designed to allow some data to be lost in transmission in exchange for faster connection speeds (Andrés et al., 2016).

Yet no matter what experience a game's engineers are attempting to create, there is a factor that is always an important concern: how players could use the game's architecture to cheat. In a survey of P2P architectures for online games, Amir Yayahvi and Bettina Kemme (2013) detail a number of ways players can cheat that are made possible by aspects of P2P architecture. Because these networks do not use centralized servers, and instead directly connect players to one another, games using P2P systems are vulnerable to methods of cheating that would not be possible in games using a peer-to-server system. These methods range from being implicitly allowed by the game's infrastructure, such as players taking advantage of the reduced authentication capabilities of P2P networks to use third-party software tools, to more explicit consequences of network limitations.

One of these more explicit infrastructure-driven methods, labelled "blind opponent" by Yayahvi and Kemme (2013, p. 34), involves players intentionally dropping outgoing updates on their actions in game, while still receiving updates from other players. Players of *For Honor* used this technique after it was discovered that they could artificially slow down their internet connection in order to gain the previously mentioned advantages bestowed to players with higher latencies. This was achieved using "lag switches": devices attached to ethernet cables that can be activated to artificially slow down a player's connection. In this way, players were able to "cheat" the game, without taking any action within the game world itself. Instead of modifying the game to gain an advantage, these players modified the infrastructure the game relied on.

Yayahvi and Kemme's (2013) classification of these infrastructure-driven player interventions as cheating raises an interesting question. The pair define cheating as something that "occurs when a player causes updates to game state that defy game rules and result in unfair advantage" (p. 33), but while the players using these methods are certainly receiving an unfair advantage over their competitors, are they actually defying the rules of the game? Mechanics and systems that players encounter within the game world itself traditionally determine digital game rules; they do not typically extend beyond that sphere (Juul, 1999). However, as theorized by Taylor (2009) in her analysis of group-play in *World of Warcraft*, the actual experience of playing an online digital game goes beyond the boundaries of the game software itself. Rather, the game exists as one node of a broader "assemblage of play" (p. 336), which is composed of multiple different actors working in tandem to create a specific, contextualized practise of play. The disparate nodes that make up this assemblage come attached with their own rules, either written or unwritten, that players are expected to follow. Breaking these rules, while not always cheating, still impacts, in some manner, the experience of playing the game. Tools such as lag-switches work in this way. As with in-game modifications and social relationships, an online game's infrastructure is a node in the broader assemblage that composes the experience of play. While not a part of the game's software, tampering with an ethernet cable or tricking network protocols still impacts the experience of both the player in question and the other players sharing that virtual space. The rules of the game can be left unbroken, but the unwritten rules surrounding the game's infrastructure—namely, that all players will interface with that infrastructure in a similar "fair" way—have been violated.

Mia Consalvo (2007) uses a definition of cheating that accounts for this assemblage of play in her book *Cheating: Gaining Advantage in Videogames*. While Consalvo (2007) initially uses a definition of cheating coined by J. Barton Bowyer, which states that "cheating is the advantageous distortion of perceived reality" (p. 5), she places far more importance on what digital game players themselves consider to be cheating. In her interviews with people who identify as game players, Consalvo (2007) found one overarching theme regarding what players considered to be cheating: the creation of a perceived unfair advantage over other players. By focusing on the definitions used by players, Consalvo framed cheating as a primarily relational concept. If players consider an action to be cheating, then it is cheating—even if that action does not technically break the rules of the game. Thus, actions that gain players an advantage through other nodes in the assemblage of play—such as players breaking social rules by lying about the usefulness of an item being offered for trade or breaking infrastructural rules by using a lag-switch to out-manoeuvre their opponents—are still considered cheating due to the creation of a perceived unfair advantage.

Using this relational understanding of cheating, it would be hard to argue that infrastructure-driven methods such as lag-switches are not cheating. Forum threads devoted to players labelling lag-switches and similar techniques as cheating are common over a wide variety of online games, and the gaming press colloquially refer to these methods as forms of cheating (Livingston, 2017). But while these infrastructure-driven methods can be considered cheating, they still differ from more traditional forms of "in-game" cheating, such as the way *Destiny* players were able to trick an artificial intelligence into falling off a cliff. These methods of "cheating the game" are alterations to the game world that explicitly break the rules of the game, while physical interventions such as lag-switches are alterations to the game's infrastructure that leave the game rules intact. Both actions are similar in that they are both forms of cheating; players view them as cheating by players and they are used to gain an unfair advantage over others. Yet, through interfacing with separate nodes of the assemblage of play, infrastructure-based cheating and "traditional cheating" remain fundamentally distinct practises.

In order to recognize this distinction, a new category should be used to delineate acts of cheating that do not actively break the rules of the game but manipulate one or more aspects of the game's infrastructure to gain an advantage over other players. These acts of "cheating the network" are separate from acts of "cheating the game" in that they require players to actively engage with the game's infrastructure—in many cases by taking action in the physical world—in order to create what James Barton Bowyer (1982) calls the "advantageous distortion of perceived reality" (p. 47). By its nature, this "cheating the network" also requires players to have some level of technical literacy surrounding the game's network technology, along with a conceptualization of this infrastructure that allows players to view it as something integral to the game's function. This type of cheating can only exist in online games that connect players using network technology; it does not require a player versus player setting. Examples such as *Destiny* players pulling their ethernet cable on an end-game boss count as "cheating the network," since the players who used that method were able to beat that encounter more easily than players who did not.

This distinction between "cheating the game" and "cheating the network" allows for the fundamentally material nature of the latter category to be recognized, opening the study of player-game interaction to a materiality-focused critical media infrastructure studies approach. Often, acts of "cheating the network" expose vulnerabilities in digital game networks that, in turn, allow for outside observers to gain a clearer picture of how these networks operate. As the following case study illustrates, using the lens of "cheating the network" allows for a more thorough understanding of how economic, political, and cultural forces shape the form that the infrastructure of a digital game will ultimately take. Additionally, by specifically focusing on instances of players "cheating the network," behaviour that was previously considered as a player-game interaction is reframed as a form of player-infrastructure interaction: interventions that go beyond the game itself and interface directly with the cables, protocols, and network architecture that connect players. This shift in perspective opens up new questions about how players conceptualize these interventions. Do players view infrastructure as a part of the game itself, or as something distinct? For them, where does the game end and the infrastructure begin?

In asking these questions, this frame also acknowledges the unusual relationship between digital game players and these networks—a relationship that subverts typical expectations of how members of the public are understood to interact with media infrastructure. By analyzing cases of game players "cheating the network," the physical manifestations of this player-infrastructure relationship can be contextualized both as an outcome of digital games as a medium, as well as a critical component of a larger media infrastructure environment.

Case study: Destiny *(2014)*

To demonstrate how the concept of "cheating the network" can be used to better understand the digital game's network infrastructure, this article will apply this framing to a case study involving Bungie's 2014 game *Destiny*. Specifically, it will use the lens provided by "cheating the network" to examine the LAN-cable exploit mentioned earlier in this article. The focus is on *Destiny* above other popular game franchises for three reasons. First, *Destiny* is a massively multiplayer online game (MMOG). As with other MMOGs, such as *World of Warcraft* or *EVE Online*, most content in *Destiny* involves multiple players simultaneously interacting with a shared, persistent world. That means when one *Destiny* player shoots an enemy or opens a treasure chest, other players in the same area see that player performing these actions in what appears to be real-time. Additionally, the changes to the game world caused by an individual player need to be uploaded to the network and propagated to other player's versions of the world; if one player damages an enemy, that same enemy appears damaged to all other players sharing that area. Maintaining this type of persistent game world, especially one where all players are meant to experience the actions of other players in a seemingly simultaneous fashion, requires extensive infrastructural support.

Second, *Destiny* makes use of a hybrid P2P network architecture to connect players. While *Destiny* uses centralized servers to ensure some aspects of the game world operate correctly, most of the in-game logic is handled using P2P networking. Peer-to-peer networks are generally faster and more responsive to player input, an important factor in a fast-paced action game such as *Destiny*. However, as mentioned earlier, a lack of server verification exposes P2P networks to a wider possible range of player-driven intervention.

Third, and perhaps most importantly, *Destiny* players are constantly finding new ways to cheat. Almost every new update and expansion to both *Destiny* and *Destiny 2* has been followed by the discovery of new exploits, most of which the popular games press has covered. Players use these to gain in-game items and rewards more quickly than intended, reducing the amount of time each player ultimately needs to invest in the game. This both creates an in-game disadvantage for players who choose not to use the exploit, and results in Bungie losing potential revenue: the more time players invest in the game, the more likely they are to spend money on expansions and in-game microtransactions. Because of this, Bungie has made it an important priority to ensure players are not able to find shortcuts, and exploits of this nature have often been patched out before other technical and systematic issues. Perhaps unsurprisingly, this has led to the *Destiny* community developing an antagonistic relationship with Bungie, with many players framing the use of exploits as a way to express frustration toward the developer's decisions. As explored by Alexander Galloway and Eugene Thacker (2007), disenfranchised groups have long used exploits as a political tool to fight asymmetric battles against more powerful opponents.[1] By using exploits to break the experience of playing *Destiny*—especially the aspects of the game players consider unfair or overly restrictive—players have found a way to reclaim power in a typically one-sided relationship.

The LAN-pulling exploit players used to defeat one of *Destiny*'s most difficult challenges exists at the nexus of these three factors. By thinking of this strategy as an instance of "cheating the network" instead of a more traditional form of cheating, these underlying factors become more visible—along with the power relations that these factors reinforce and are reinforced by.

On December 9, 2014, Bungie released *Destiny*'s second raid, entitled Crota's End. Originating from the multiplayer text-based games of the early 1990s, raids are cooperative in-game activities that task MMOG players with navigating through a dungeon and defeating a final boss. They are typically challenging and time-consuming, meant to test both players' individual skill and their ability to communicate effectively with teammates. Fittingly, they also offer the game's most powerful weapons and armour as rewards for completion.

Upon release, players discovered that Crota's End was indeed difficult, though not necessarily by design. While considered by the community to be one of *Destiny*'s easier raids in a mechanical sense, the raid's final fight against the titular Crota had a number of recurring bugs that caused frustration among players. Smaller enemies would behave erratically, crucial items would fall through the floor, and Crota himself would occasionally stop taking damage altogether. These bugs, which were caused both by issues with the game's network architecture and errors in artificial intelligence, made the complicated multistep fight almost impossible for some players. "One of these things has happened almost every attempt we have run, with only about 1 in 10 of our wipes being because of issues on our end," wrote one player in a post on a *Destiny* message board (DoctorKoolMan, 2015). Yet despite vocal complaints, Bungie never addressed many of these bugs, and players report that some still persist in the raid's current form. In a forum thread created in March of 2017, three years after the release of the raid, players were still venting their frustration. "It really is still VERY bugged and I know it cost us the challenge at least a couple of times. I'll be happy just to finish it once for the emblem and never look at Crota again," wrote one player (Dirty8Speciall, 2017). "They never got round to fixing it for the first 2 years. I very much [doubt] they'll bother now," wrote another (DeadlyMenace, 2017).

Perhaps because of frustration with these bugs, many *Destiny* players quickly adopted an unconventional method of defeating Crota. To complete the encounter as intended by Bungie, players would have to perform a series of actions to force Crota into a vulnerable state, represented by the character kneeling. Once Crota was vulnerable, players had a small window to deal damage to him before he stood up, at which point the process had to be repeated. As mentioned earlier, players discovered that if the "host" of the team disconnected from *Destiny* while Crota was kneeling, the boss would be permanently stuck in this vulnerable position until the end of the fight. The team could then wait for the host player to reconnect and quickly finish the raid without much trouble. These intentional disconnections could be accomplished through players either physically removing the ethernet cable from their game consoles or by force quitting the game using options in the console's menu. The imagery, however, of pulling the LAN cable to kill Crota quickly came to define the technique. By using this technique, players were able to functionally skip the challenging final encounter of Crota's End, while still receiving the rewards for completing the raid. One player on the Destiny subreddit defended his use of this exploit: "people just want easy loot and don't want to waste 6 hours wiping" (Kharrz, 2014).

While there was some debate in the *Destiny* community over whether or not this act was cheating (with arguments that it was "not technically cheating" [Saikoro, 2014] due to the exploit not breaking the game rules), the majority of player voices seemed to agree that those who chose to "cheese" the encounter gained an advantage over those that wanted "to do it the right way" (Amytrixter, 2014). For the purposes of this article, this perceived unfair advantage makes the Crota exploit constitute a form of cheating, and its use of infrastructure external to the game makes this an act of "cheating the network." By framing the Crota exploit in this way, this act of cheating the network can be seen as a sort of access point for a scholarly intervention into the system of infrastructure Bungie used to support *Destiny*'s online gameplay. It is now possible to ask the question: what part of *Destiny*'s infrastructure made the Crota exploit possible?

In a presentation for the 2015 Game Developers Conference, Bungie engineer Justin Truman explained how specifically timed disconnections were able to freeze Crota. *Destiny*, similar to any MMOG, has to constantly maintain and update a simulation of a shared game world. A computer needs to keep track of the position and status of all the objects in the world and ensure that any changes players or AI cause to these objects are kept consistent with changes made by other entities. For more linear activities such as Crota's End, this also includes keeping track of player progression: which doors players have opened, which puzzles they have solved, and which bosses they have defeated. Because *Destiny* uses a hybrid P2P network, Bungie had to decide which parts of the shared game world to simulate on a centralized server, and which parts to simulate using a P2P "host" architecture. The latter system chooses one player in any given game area to be the "host," and has the host's console manage and update the world simulation. Other players' consoles then send and receive updates to the host player, instead of to a centralized server.

While a host system helps remove latency between player input and in-game action, it also allows for a singularly disruptive event: the potential disconnection of the host player. When this occurs (either intentionally or unintentionally on behalf of the host), the game has to select a new host and transfer the simulation authority to the new host's console. This process, however, takes time, and in that time players will continue to make changes to the game world. As described by Truman (2015):

> … that new host's simulation state will not be identical to the old host. Not only may objects be in slightly different states, she might not have all the same objects instantiated as the old host. She may have prematurely deleted some objects. And this can cause some pretty severe experiential bugs — in the worst case, it can completely break activity script progression. (p. 60)

This "worst case" is exactly what happened in Crota's End. While Bungie attempted to prevent these types of errors by using centralized servers (called "activity managers") to independently track player progress through raids and other activities, the developer wanted these servers to only be working with "mission critical" information: whether enemies are alive or dead, whether doors are opened or closed, and whether quest objectives have or have not been completed. In order to maintain low in-game latency, as little data as possible was to be sent between players and centralized servers. Activity managers did not track information about the game world that Bungie decided was not mission critical, such as the specific states of AI characters, and it was put at risk of being lost during the transfer to a new player host.

While this approach to host transfers worked for most activities in *Destiny*, the specific state of an AI character was, in fact, "mission critical" information in the final battle of Crota's End. No one at Bungie thought to program the activity managers to keep track of the time remaining in Crota's vulnerability state, which resulted in this information not being properly transferred to the new host when the old host disconnected. Thus, when the host disconnected, Crota remained trapped in his vulnerable state indefinitely.

This oversight, and ultimately the exploit itself, emerged because of the decisions made by Bungie when designing the network architecture of *Destiny.* Specifically, this exploit was caused by the decision to prioritize connection speed over reliability. Not only did this choice lead to the adoption of a P2P network but also to the Spartan nature of the centralized server system the company used in an attempt to mitigate the consequences of that P2P network.

This is not to say that Bungie's choice was the wrong one. A version of *Destiny* that only uses centralized servers to simulate shared game worlds would have constant latency problems, a situation that would likely be even more controversial than the occasional exploit. However, while Bungie did not necessarily make the wrong choices when designing *Destiny*'s network infrastructure, this example does show how those high-level choices ultimately shaped the ways in which players were able to interact with the game. Players were able to freeze Crota because a fundamental aspect of *Destiny*'s P2P network (the reliance on a player host) allowed for the possibility of a disastrous edge-case (player host disconnection), which Bungie tried to solve (using activity manager scripts running off of centralized servers) while still maintaining fast connection speeds (strictly limiting the information sent between players and centralized servers).

Looking at the Crota exploit through the lens of "cheating the network" has revealed these choices, and allows the economic, cultural, and political pressures that led to these decisions to be interrogated. Economically, having a system that minimized the amount of information dedicated servers needed to track benefitted Bungie (and its publisher at the time, Activision), by lowering the number of servers needed to maintain *Destiny*'s online network. Truman (2015) directly states in his presentation that one of the benefits of the "activity manager" being as small as possible was the reduction of server numbers, so the existence of the Crota exploit can be in part explained by the economic motivations of Bungie and its publisher. Other factors can also be identified, such as the cultural expectation that a first-person shooter game such as *Destiny* processes information quickly enough that the action appears instantaneous. The wider infrastructural ecosystem *Destiny* interfaced with should also be seen as an influence on the choices Bungie made, as the game needed to make use of existing internet infrastructure to connect players from across continents. The technical limitations and physical constraints presented by this existing network make sending large amounts of information difficult and time consuming, a factor that influences all games that make use of the internet (Armitage et al., 2006).

By having player hosts disconnect at precisely the right time, *Destiny* players were able to take advantage of a structural weakness in the game's network and, in doing so, expose the forces acting upon the creation and implementation of the infrastructure built to maintain this network. Fittingly, Bungie did not fix this exploit by patching the software-level code that makes up Crota's End. Instead, it gave the activity manager's scripts responsibility over tracking Crota's vulnerability state. In a way, the game was not patched at all—the network was.

Conclusion

When *Destiny* players learned that pulling out their ethernet cables could help them more easily defeat a boss, *Kotaku* writer Schreier (2015) described this action as cheating. Those players were not "cheating the game." Instead, they were "cheating the network," taking advantage of the cables, network protocols, and other structures used to support online digital games. These systems make up the infrastructure of online games that, like all media infrastructures, are essential to the operation of the medium they support. In part due to the way this infrastructure impacts the experience of gameplay, digital game players have learned to directly engage with these networks in order to gain advantages in online games.

By distinguishing these acts from traditional, game-level cheating, the material nature of player-infrastructure interactions becomes apparent. Future work along these lines could apply this concept of "cheating the network" to the analysis of specific case studies, examining instances of players moving beyond their games and intervening with infrastructure. This approach uses the vulnerabilities in digital game networks made visible by acts of "cheating the network" to better understand the choices and compromises that went into the formation of these networks, which, in turn, allows for the application of critical interrogations of the economic, political, and cultural forces acting upon those choices.

In analyzing this behaviour under a critical material lens, it is also possible to better understand the unusual relationship digital game players have with media infrastructure and the factors that contributed to the growth of this relationship. While not explored in the case study presented here, this potential avenue for "cheating the network" could seek to identify the aspects of digital games and digital game culture that have resulted in a greater infrastructural awareness among players of online digital games, and perhaps even attempt to replicate this heightened awareness in other groups of people. Future work along these lines could also seek to connect acts of "cheating the network" with other historical examples of users engaging with and disrupting infrastructure for their own ends, creating a historical continuity in line with the work of scholars such as Tung-Hui Hu (2015). In an age where the public is largely unaware of the media infrastructures that connects it, people who play digital games seem to be running against the current. Perhaps in "cheating the network" there lies a key to unlocking a more nuanced understanding of infrastructural literacy.

Note

[1] In writing about exploits, it was important to acknowledge the work done on this subject by scholars in the field of network theory, in particular that of Alexander Galloway and Eugene Thacker (2007). However, while this article briefly touches upon the political usefulness of exploits in resisting dominant systems of power, there remains much to explore about the capacity of exploits to expose previously unseen political, economic, and cultural forces acting upon the form of media infrastructure.

Video games

Destiny (2014), Bungie
For Honour (2017), Ubisoft
World of Warcraft (2004), Blizzard

References

Alexandria, Heather. (2017). For honor players claim to be troubled by lag. *Kotaku.* URL: https://kotaku.com/for-honor-players-claim-to-be-troubled-by-lag-1792638452 [February 25, 2019].

Andrés, Cristian, López, Melo, José, Octavio, Parra, Salcedo, & Torres, Andrés Gallego. (2016). Networks and their traffic in multiplayer games. *Revista Cientifica, 1*(24), 100–109.

Armitage, Grenville, Claypool, Mark, & Branch, Philip. (2006). *Networking and online games: Understanding and engineering multiplayer internet games.* West Sussex, UK: Wiley.

Amytrixter. (2014). No title [Message 14]. *Reddit.* URL: https://www.reddit.com/r/DestinyTheGame/comments/2qq8c9/this_has_been_bugging_me_lately/ [February 25, 2019].

Bowker, Geoffrey C., Baker, Karen, Millerand, Florence, & Ribes, David. (2010). Toward information infrastructure studies: Ways of knowing in a networked environment. In Jeremy Hunsinger, Lisbeth Klastrup, & Matthew Allen (Eds.), *International handbook of internet research* (pp. 97–117). Dordrecht, NL: Springer Netherlands.

Bowyer, James Barton. (1982). *Cheating.* New York, NY: St Martin's Press.

Conaway, Evan P. (2017). Play as theory, object, and analytic. *American Anthropologist.* URL: http://www.americananthropologist.org/2017/11/27/from-the-archives-play-as-theory-object-and-analytic-by-evan-p-conaway/ [February 25, 2019].

Consalvo, Mia. (2007). *Cheating: Gaining advantage in videogames.* Cambridge, MA: MIT Press.

Chung, Jaeyong, & Gardner, Henry J. (2012). Temporal presence variation in immersive computer games. *International Journal of Human-Computer Interaction, 28*(8), 511–529.

DeadlyMenace. (2017). No title [Message 10]. *Bungie.* URL: https://www.bungie.net/en/Forums/Post/223909251?sort=0&page=0 [February 25, 2019].

Dirty8Speciall. (2017). No title [Message 20]. *Bungie.* URL: https://www.bungie.net/en/Forums/Post/223909251?sort=0&page=0 [February 25, 2019].

DoctorKoolMan. (2015). crota too buggy to fight [Message 1]. *GameFAQs.*URL: https://gamefaqs.gamespot.com/boards/704532-destiny/71103598 [February 25, 2019].

Dourish, Paul. (2015). Protocols, packets, and proximity: The materiality of internet routing. In Lisa Parks & Nicole Starosielski (Eds.), *Signal traffic: Critical studies of media infrastructures* (pp. 184–204). Champaign, IL: University of Illinois Press.

Galloway, Alexander R., & Thacker, Eugene. (2007). *The exploit: A theory of networks.* Minneapolis, MN: University of Minnesota Press.

Hu, Tung-Hui. (2015). *A prehistory of the cloud.* Cambridge, MA: MIT Press.

IPetitions. (2017). For honor – dedicated servers – no purchase otherwise. *iPetitions.* URL: https://www.ipetitions.com/petition/dedicated-servers-for-honor-no-purchase [February 25, 2019].

Juul, Jesper. (1999). A clash between game and narrative. *Jesper Juul.* URL: https://www.jesperjuul.net/thesis/ [February 25, 2019].

Kharrz. (2014, December 21). No title [Message 2]. *Reddit.* URL: https://www.reddit.com/r/DestinyTheGame/comments/2pyld6/sga_crota_cheese_is_cheating_and_heres_why/ [February 25, 2019].

Levin, Boaz, & Jeffery, Ryan. (2016). Lost in the cloud: The representation of networked infrastructure and its discontents. *Spheres.* URL: http://spheres-journal.org/lost-in-the-cloud-the-representation-of-networked-infrastructure-and-its-discontents-2/ [February 25, 2019].

Liebl, Matt. (2014). Destiny update 1.0.2.3 released: Finally fixes Atheon exploit in Vault of Glass. *Gamezone.* URL: http://www.gamezone.com/news/destiny-update-1-0-2-3-released-finally-fixes-atheon-exploit-in-vault-of-glass [February 25, 2019].

Livingston, Christopher. (2017). Battlegrounds patch tackles 'lag switch' cheaters by freezing them in place. *PC Gamer.* URL: http://www.pcgamer.com/battlegrounds-update/ [February 25, 2019].

Mosco, Vincent. (2014). *To the cloud: Big data in a turbulent world.* Boulder, CO: Routledge.

Newell, Adam. (2017). For Honor is getting an international tournament with a $10,000 prize pool. *Dot Esports.* URL: https://dotesports.com/general/news/for-honor-international-15699 [February 25, 2019].

Parks, Lisa. (2015). 'Stuff you can kick': Toward a theory of media infrastructures. In Patrik Svensson & David Theo Goldberg (Eds), *Between humanities and the digital* (pp. 355–374). Cambridge, MA: MIT Press.

Parks, Lisa, & Starosielski, Nicole. (2015). Introduction. In Lisa Parks & Nicole Starosielski (Eds.), *Signal traffic: Critical studies of media infrastructures* (pp. 1–25). Champaign, IL: University of Illinois Press.

SA1KoRo. (2014). No title [Message 23]. *Reddit.* URL: https://www.reddit.com/r/DestinyTheGame/comments/2qq8c9/this_has_been_bugging_me_lately/ [February 25, 2019].

Schreier, Jason. (2015). Destiny's latest exploit: Pulling out your LAN cable. *Kotaku.* URL: https://kotaku.com/destinys-latest-exploit-pulling-out-your-lan-cable-1677068155 [February 25, 2019].

Star, Susan Leigh, & Ruhleder, Karen. (1996). Steps toward an ecology of infrastructure: Design and access for large information spaces. *Information Systems Research, 7*(1), 111–134.

Starosielski, Nicole. (2015). *The undersea network.* Durham, NC: Duke University Press.

Taylor, T.L. (2009). The assemblage of play. *Games and Culture, 4*(4), 331–339.

Truman, Justin. (2015). Shared world shooter. *GDC Vault.* URL: https://www.gdcvault.com/play/1022247/Shared-World-Shooter-Destiny-s [February 25, 2019].

Yahyavi, Amir, & Kemme, Bettina. (2013). Peer-to-peer architectures for massively multiplayer online games. *ACM Computing Surveys, 46*(1), 1–51.