L'AGENCEMENT DE LA TRICHE

Aborder la triche dans les MMORPG comme un imbroglio

Stefano DE PAOLI et Aphra KERR

DOI: 10.3917/res.173-174.0235

Le texte qui suit est la traduction d'un article original paru en 2010 dans le numéro 16 de la revue en ligne The Fibreculture Journal "Counterplay : Gaming, Cheating and Control", numéro coordonné par Thomas Apperley et Michael Dieter[1]*. Aphra Kerr, chercheur en sociologie et enseignante à l'Université Nationale d'Irlande, Maynooth, travaille depuis de nombreuses années sur les industries culturelles, et particulièrement sur la régulation, la production et l'usage de jeux vidéo. Avec son ouvrage paru en 2006 chez Sage Publication, The Business and Culture of Digital Games: Gamework and Gameplay, elle propose d'aborder les jeux sur support numérique dans leur complexité, c'est-à-dire comme des artefacts socialement négociés, qui émergent dans des configurations politiques, culturelles, économiques, techniques et sociales particulières. Membre fondatrice de l'une des principales associations de recherche sur les jeux vidéo : la Digital Game Research Association (DiGRA), son travail se distingue au sein des game studies en s'intéressant autant aux contextes de production qu'à ceux des usages des jeux, et en mobilisant les avancées théoriques de la sociologie des médias, des études culturelles et de la sociologie des sciences et des techniques.*

Cette dernière perspective est celle qui encadre le plus le travail empirique et théorique qu'elle mène avec Stefano de Paoli[2]*, chercheur dont les travaux s'intéressent aux relations entre technique et société, et notamment aux rôles de régulation d'artefacts textuels tels que les licences logicielles. Leur collaboration sur l'étude des phénomènes conflictuels dans les MMORPG, et plus particulièrement sur la triche a donné lieu à plusieurs publications qui offrent des perspectives originales sur les relations entre développeurs, techniques et joueurs. Celle qui suit s'intéresse particulièrement à la façon dont le concept d'agencement peut être mobilisé pour aborder d'une manière qui ne soit pas essentialiste le phénomène de la triche dans les jeux en ligne.*

---

1. Traduit de l'anglais par Vinciane Zabban. Je remercie les auteurs pour leur collaboration ainsi que la revue en ligne *Fibreculture* qui a autorisé cette publication. Je remercie également Bruno Vétel et Ashveen Peerbaye pour leur relecture. Le texte a fait l'objet de coupes pour les besoins de cette traduction et il peut être consulté dans sa version originale sur le site de la revue The Fibreculture Journal (http://fibreculturejournal.org).

2. Stefano de Paoli était post-doctorant à l'Université Nationale d'Irlande, Maynooth, de juin 2008 à décembre 2010 ; il travaille actuellement pour la Fondation Ahref (Italie).

La question que nous posons dans cet article est la suivante : comment décrire la triche dans les jeux de rôle en ligne massivement multijoueurs (Massive Multiplayer Online Role-Playing Games : MMORPG) ? Il est important de clarifier d'emblée que ce qui est en jeu ici est la manière dont on étudie le phénomène de la triche, et comment on le conceptualise dans le cadre de recherches sur les MMORPG. Nous insistons en particulier sur la différence qu'il y a entre le fait de définir, voire de réduire, un phénomène en le rapportant à ses caractéristiques intrinsèques, et une approche qui s'intéresse aux processus qui le génèrent (cf. Latour, 1987, 2005 ; Lash, 2002 ; DeLanda, 2002, 2006).

L'entrée par cette question de recherche se justifie par le fait qu'une part importante de la littérature a réduit la triche dans les jeux en ligne à un ensemble de traits caractéristiques, pour l'appréhender comme l'ensemble des actions à travers lesquelles certains joueurs altèrent le jeu afin d'obtenir un avantage déloyal sur d'autres. Nous suggérons au contraire que la triche devrait être conceptualisée non seulement à partir du comportement des joueurs, mais en tenant compte des relations réciproques qui s'établissent concrètement entre divers éléments composant les MMORPG. Nous apportons une perspective nouvelle sur la triche dans les MMORPG, en suggérant qu'elle résulte d'un processus dynamique et des relations réciproques d'une série d'éléments.

Le phénomène de triche est étudié dans cet article en mobilisant le concept d'agencement, tel que le propose DeLanda (2002, 2006) à la suite de Deleuze et Guattari (1987)[3]. Ce concept repose sur une posture réaliste qui insiste sur le fait que les phénomènes sociaux et naturels doivent être compris comme les résultats dynamiques de relations contextuelles et historiques entre éléments concrets, et non pas à travers une liste exhaustive de traits essentiels ou des classifications intemporelles. Dans cet article, nous tenons compte des éléments suivants des MMORPG et de la manière dont ils sont reliés (tout en étant conscients que cette liste n'est pas nécessairement définitive) : l'architecture, le code et les documents juridiques du jeu. De plus, nous nous focalisons sur la façon dont ces éléments s'articulent avec les joueurs, les entreprises de jeu, mais aussi avec les entreprises qui offrent des services de triche. Selon nous, la triche possède une frontière mobile et perméable où ces différents éléments, et à travers eux les stratégies des joueurs et des

3. NdT. Le concept d'agencement est traduit en anglais, dans les écrits de DeLanda, et dans la version originale de ce texte par *assemblage*. Nous faisons ici le choix de restituer le terme employé originellement par DeLanda, Deleuze et Guattari.

entreprises, s'affrontent et/ou coopèrent – toujours en relation les uns avec les autres – dans un processus de stabilisation et de déstabilisation de la définition de ce qu'est tricher dans un MMORPG. Notre argument est principalement soutenu par des illustrations empiriques qui proviennent d'une recherche en cours sur le jeu en ligne Tibia (http://www.tibia.com), un MMORPG médiéval fantastique en deux dimensions, développé et distribué par CipSoft depuis 1997. Le jeu est disponible sur plus de 70 serveurs en Allemagne et aux États-Unis et on estime le nombre de joueurs de Tibia à 300 000.

L'approche par l'agencement cherche également à identifier ce qui est défini comme la structure d'un espace des possibles (DeLanda, 2002) afin de distinguer ce qui est possible en principe dans un agencement (le virtuel[4]) et ce qui est effectivement actualisé. Le concept d'agencement s'est avéré d'une utilité majeure dans notre quête d'une ressource théorique à même de saisir les dimensions empiriques et sociotechniques des négociations et des luttes de pouvoir autour de la triche dans les MMORPG. Nous pensons qu'adopter ce concept nous permettra de mettre au jour les dynamiques impliquées dans la dialectique entre le virtuel et l'actuel de la triche dans les MMORPG.

Nous sommes convaincus qu'une meilleure compréhension du caractère processuel de la triche dans les MMORPG – entendue comme un agencement – est utile non seulement en soi, mais aussi pour mieux appréhender les concepts associés de contre-jeu (*counterplay*) ou de jeu transgressif (*transgressive play*) (Aarseth, 2007). Nous discuterons en particulier le concept de contre-jeu[5] en le mettant en relation avec les aspects virtuels et actuels de la caractérisation de la triche comme agencement dans les MMORPG. Le concept de contre-jeu implique de penser l'activité de jeu comme la négociation de relations de pouvoir exercées par la matérialité du logiciel et une série d'autres artéfacts. Notre perspective sur la triche nous conduit à explorer non seulement la série d'artéfacts et d'acteurs qui sont impliqués dans l'agencement des MMORPG, mais aussi la renégociation continuelle des relations au sein de cet agencement.

---

4. Le mot virtuel n'est pas utilisé ici dans le sens qu'il a dans l'expression « réalité virtuelle », mais dans celui de champ des possibles (cf. la section « Théorie de l'agencement » de cet article).

5. NdT. Le concept de contre-jeu (*counterplay*) constitue la thématique centrale du numéro de la revue *Fibreculture* dans lequel est paru originellement cet article. Le numéro appelait les auteurs à réfléchir au potentiel de la notion de « contre-jeu » pour l'analyse des controverses qui encadrent certaines actions rebelles ou innovations qui émanent des communautés de joueurs.

L'organisation du texte est la suivante : premièrement, nous présentons les enjeux de travaux sur la triche et mettons en discussion les définitions les plus répandues de la triche dans les MMORPG ; deuxièmement, nous présentons le concept d'agencement qui est à l'origine de notre approche ; troisièmement, nous apportons des illustrations de la façon dont la triche peut apparaître comme le produit de l'agencement des MMORPG ; quatrièmement, nous précisons notre contribution au concept de « contre-jeu ». Enfin, pour conclure, nous élaborons une nouvelle définition de la triche appuyée par nos résultats.

DÉFINIR LA TRICHE : LÀ EST LE PROBLÈME

Les MMORPG sont des produits à succès de l'industrie des jeux vidéo[6] dans lesquels les joueurs investissent un monde virtuel persistant (Bell, 2009) qui nécessite le déploiement par les développeurs du jeu d'un support continu à la clientèle (Kerr 2006). Les MMORPG sont aussi des systèmes techniques sophistiqués qui reposent la plupart du temps sur une architecture client-serveur (voir la figure 2) et un code informatique complexe. Les MMORPG sont enfin des mondes « profondément sociaux » (Castronova, 2005 ; Taylor, 2006), dans lesquels des milliers de joueurs coopèrent, rivalisent et échangent en ligne.

De nombreuses études ont relevé le fait que la complexité sociotechnique des MMORPG était susceptible d'ouvrir ces jeux à un ensemble de pratiques perturbatrices (pour un aperçu, cf. ENISA, 2008), telles que l'arnaque (Bardzell et al., 2007), le harcèlement (Foo & Koivisto, 2004), ou des conflits de nature sociale (Smith, 2004). Notre recherche s'intéresse en particulier aux pratiques et aux conséquences de la triche pour ces jeux, et pour des environnements virtuels de manière plus générale. Cet article est issu du travail mené dans le cadre d'un projet de recherche interdisciplinaire composé de chercheurs en informatique et en sciences humaines, axé sur la conception de services et d'application pour le futur d'Internet. Notre recherche sur la triche se veut contribuer à une compréhension fine des ressorts sociaux de la triche dans les MMORPG en particulier, et des comportements sociaux dans les environnements en ligne plus généralement.

6. Pour obtenir des données chiffrées sur l'usage des principaux MMORPG, se référer à http://www.mmogchart.com.

Comprendre les pratiques de triche est d'une importance capitale pour appréhender la pratique des jeux en ligne (Consalvo, 2007). En effet, la triche dans un MMORPG est un phénomène hautement controversé qui mérite une attention particulière, dans la mesure où elle est perçue par les développeurs, les éditeurs et les joueurs comme une menace pour l'équilibre social et la viabilité économique d'un jeu. Pour d'autres néanmoins, tricher peut être justifié par le fait de générer une quantité importante de monnaie réelle et virtuelle, ou de pouvoir s'élever plus rapidement dans les classements du jeu.

Chaque nouveau projet de recherche sur la triche dans les MMORPG doit se confronter aux définitions les plus courantes de ce phénomène. Il existe plus précisément deux genres principaux de littérature sur la triche dans les jeux vidéo hors ligne et en ligne : une littérature qui émane des sciences techniques et informatiques (cf. Yan & Randell, 2005) et une littérature qui émane des *media studies* et des *game studies* (cf. Consalvo, 2007). Nous avons détaillé ailleurs (de Paoli & Kerr, 2010) le fait que le premier type de littérature s'intéressait principalement à la triche comme phénomène résultant de faiblesses dans la conception en matière de sécurité, alors que le second insiste davantage sur ses dimensions culturelles et sur l'idée que la triche est souvent un révélateur du pouvoir d'action des joueurs. Bien que ces deux types de littérature renvoient à des directions et à des méthodes manifestement distinctes, elles partagent souvent la même définition de la triche.

Parmi les définitions les plus répandues de la triche, on peut citer celle qui est donnée par Salen et Zimmerman (2003) dans leur ouvrage sur la conception de jeux vidéo : « Le tricheur commet de manière subreptice des actes qui ne sont pas proscrits par les règles afin d'en tirer un bénéfice. » Si l'on se fie à Parker (2007, p. 2) et à son travail sur la triche dans les jeux vidéo, « nous pouvons convenir qu'un tricheur triche dans le but d'avoir de meilleures chances d'arriver à ses fins, quelles qu'elles soient ». Brooke et al. (2004), en travaillant sur le bien-être des « Sociétés virtuelles » avancent que la triche peut être définie comme « le fait d'obtenir un avantage déloyal sur d'autres participants ». Smith (2004, p. 5), en observant les conflits sociaux dans les jeux multijoueurs en ligne, affirme pour sa part : « typiquement, un comportement qualifié de triche donne au tricheur un avantage déloyal sur ses adversaires et/ou va à l'encontre de l'esprit du jeu ». On pourrait aisément rallonger la liste des publications qui partagent des définitions similaires de la triche (cf. Yan & Choi, 2002 ou Webb et Soh, 2007).

Si nous laissons pour l'instant de côté quelques exceptions[7], nous pouvons sans mal conclure de ces exemples que la majorité de la littérature définit la triche comme une action par laquelle un individu obtient un avantage déloyal. Voici donc le « trait essentiel » des activités de triche, sans lequel le phénomène ne serait pas ce qu'il est : l'obtention d'un avantage déloyal sur d'autres joueurs. Autrement dit, si aucun avantage déloyal n'est obtenu au travers d'actions particulières, nous n'avons pas affaire à de la triche, mais à quelque chose d'autre.

Nous sommes conscients du fait que, tout particulièrement dans les *media studies*, la discussion sur la triche prend en compte et interroge le caractère controversé de ce phénomène[8]. Le travail qui est, par exemple, mené par Consalvo met très clairement en avant le fait que la définition de ce qu'est tricher est culturellement négociée par les joueurs, les tricheurs et l'industrie antitriche. Dans le même temps cependant, l'ouvrage de Consalvo contribue fortement à une appréhension de la triche comme « un avantage déloyal » : le chapitre 4 dans son intégralité ainsi que la conclusion du chapitre 7 traitent notamment de la manière dont les joueurs négocient la signification de la triche entendue comme « obtention d'un avantage déloyal ».

Les travaux qui fournissent des classifications et des typologies de la triche (Yan & Randell, 2005 ; Webb & Soh, 2007) adoptent également une perspective essentialiste, dans la mesure où la triche y est caractérisée à travers l'énumération, dans des classifications décontextualisées, des différentes catégories d'abus et de motifs de triche. Pour les MMORPG, cela va de l'usage de logiciels qui interfèrent avec le client du jeu, à l'exploitation de failles de conception et de bugs du jeu, voire même l'ingénierie sociale.

Les traits essentiels de la triche

L'expression « traits essentiels » joue un rôle crucial dans notre argumentation. En effet, nous pensons que les définitions courantes de la triche induisent une perspective essentialiste selon laquelle ce qui constitue ou ne constitue pas un acte de triche est défini *ex ante*. Adopter une telle définition reviendrait à disposer par avance d'une explication causale ou d'une interprétation de la

7. L'une des alternatives est le travail mené par Kücklich (2007, 2009), qui perçoit la triche comme une ressource méthodologique pour la recherche sur les jeux.
8. Voir par exemple Kücklich (2005).

triche qui anticipe les dynamiques concrètes à travers lesquelles le phénomène se déroule. En fait, nous saurions déjà, avant même d'entamer notre enquête empirique, ce qu'il faudrait y trouver : tout ce qui pourrait procurer un avantage déloyal aux joueurs, et éventuellement les motivations qui pourraient pousser les joueurs à tricher. Contre ces classifications communes qui se concentrent uniquement sur un ensemble réduit de traits essentiels, et pour dépasser une définition qui aborde la triche simplement comme ce qui procure « un avantage déloyal », nous proposons de nous concentrer sur les processus relationnels qui s'établissent entre les éléments qui composent les MMORPG, et à partir desquels émerge la triche.

Nous pensons que la limite des définitions et classifications courantes de la triche se situe précisément en ce point. Adopter une approche processuelle de la triche nous permet d'inclure dans nos recherches et dans notre argumentation une plus grande diversité d'éléments ainsi que leurs dynamiques relationnelles. Nous ne pouvons effectivement isoler les traits caractéristiques de la triche tout le reste, car ce sont les relations réciproques entre éléments qui priment. Par conséquent, nous pensons que la triche devrait être considérée comme le produit des relations tissées entre différents éléments, y compris ceux qui ne sont pas directement à l'origine d'un avantage déloyal. Il nous faut désormais appliquer cette approche conceptuelle à la triche dans les MMORPG.

La théorie de l'agencement

Nous devons tenir compte d'au moins deux contraintes : d'abord le fait que concevoir la triche nécessite le recours à une approche non essentialiste, et ensuite le fait que nous avons besoin d'un concept qui puisse saisir à la fois les relations entre des éléments variés et ce qui découle de ces relations. Un bon candidat pour faire face à ces deux problèmes est l'approche connue sous le nom de théorie de l'agencement (DeLanda, 2002, 2006)[9].

Selon DeLanda (2006), le concept d'agencement permet de penser les relations entre un tout et ses parties. Il propose une manière de conceptualiser dans le même temps les relations qui existent entre des éléments et ce que ces relations produisent. DeLanda (2006) précise par ailleurs que les relations qui

9. Une autre approche aurait pu être celle de la théorie de l'Acteur-Réseau ou ANT (Latour, 2005). Pour cet article, il nous semble préférable de mobiliser la théorie de l'agencement, qui n'impose pas, comme l'ANT, d'adopter la perspective de certains acteurs (c'est-à-dire les ingénieurs).

existent entre les éléments d'un agencement ne sont pas nécessaires, ce qui serait le cas dans un « système ». En effet, le concept de système, dans les sciences naturelles comme dans les sciences humaines est lui aussi fondé sur la conception des relations entre éléments qui forment un tout. Les relations entre les différentes parties d'un système sont nécessaires. Par conséquent, la défaillance de l'une de ces relations conduit à celle du système entier. Dans les sciences sociales, le concept de « système social » établit un parallélisme avec les systèmes biologiques, selon lequel des institutions sociales – la religion, l'économie – sont nécessaires à l'intégration des sociétés (Parsons, 1951). Le manque de repères éthiques peut, par exemple, introduire l'anomie dans une société et entraîner la désintégration du système social (Durkheim, 1951).

Dans la théorie de l'agencement, les relations entre les parties sont pensées différemment : les éléments sont intégrés au tout par des relations contingentes (non nécessaires). En d'autres termes, les relations peuvent changer à tout moment et les parties peuvent se défaire d'un agencement et en rejoindre d'autres, y compris en y tenant des rôles distincts. Cela invite à appréhender les relations entre les éléments depuis une perspective historique et empirique, davantage que d'un point de vue purement théorique, comme pour le concept de système. Les rôles et les relations entre les éléments qui composent un agencement ne peuvent donc être déduits a priori, mais dépendent de la « structuration de l'espace des possibles ». Cette notion indique, selon DeLanda, que les compétences et les rôles d'un agencement et des éléments qui le composent ne sont pas donnés d'avance. Par conséquent, cette structure de l'espace des possibles est un espace virtuel, un ensemble de relations qui n'ont pas encore été actualisées en quelque chose de concret. C'est pourquoi la façon dont les éléments de l'agencement sont liés et ce que cet agencement produit émergent au travers de processus empiriques et historiques.

Comment alors rendre compte des dynamiques empiriques d'un agencement ? La section suivante traite de ce problème.

Les dimensions de l'agencement

Un agencement est conceptualisé en tenant compte de deux dimensions fondamentales (DeLanda, 2006) : l'axe matériel/expressif et l'axe territorialisation/déterritorialisation. Ces dimensions réfèrent au rôle et aux potentiels particuliers qu'un élément peut faire jouer lorsqu'il entre en relation avec d'autres. Ces rôles peuvent aussi apparaître comme des compositions : les

mêmes éléments peuvent faire jouer un ensemble de potentiels différents.

Sur le premier axe, le potentiel va du niveau le plus matériel au plus expressif. Delanda (2006) semble suivre Deleuze et Guattari (1987) lorsqu'il compare l'axe matériel/expressif de l'agencement à la différence qui existe entre la série de lois qui régit l'ordre (discipliner) et celle qui l'exerce matériellement (punir). Deleuze (1984) montre comment dans le *Surveiller et punir* de Foucault (1977), les relations entre la loi pénale (nommée par Deleuze « machine abstraite »), et l'exercice concret de la loi (la « machine concrète » de la prison moderne), illustrent effectivement la dialectique entre le matériel et l'expressif dans un agencement. Pour Deleuze et Guattari (1987, p. 88), cette dimension représente donc l'articulation entre les niveaux sémiotiques (p. ex. la description d'un corps) et matériels (p. ex. le corps lui-même et la façon dont il est traité) d'un agencement. Précisons par ailleurs que les relations entre les potentiels matériels et expressifs sont symétriques : chacun peut influencer l'autre. L'opposition entre potentiels fonctionnels et non fonctionnels est en cela remise en question, par exemple dans le rapport qui existe entre l'infrastructure d'une ville (matériel) et sa ligne d'horizon (expressif) (Harman, 2008). Certains éléments d'un agencement comme une ville peuvent renvoyer à ses potentiels matériels (plus fonctionnels) comme expressifs (non fonctionnels).

La seconde dimension de l'agencement concerne les capacités de territorialisation et de déterritorialisation de ses éléments. Selon DeLanda (2006, p. 13), la territorialisation est un processus qui « augmente l'homogénéité interne de l'agencement » et induit une stabilisation des relations dans celui-ci. À l'inverse, la déterritorialisation affaiblit l'homogénéité de l'agencement et déstabilise les relations entre ses éléments.

L'axe territorialisation/déterritorialisation, selon DeLanda, évoque généralement une dynamique spatiale, comme celle qui distingue une communication en face à face (territorialisation) d'une communication médiatisée (déterritorialisation). Un autre exemple est celui d'une organisation qui peut opérer tantôt au sein de bâtiments spécifiques (territorialisation), tantôt à l'écart (déterritorialisation). Cette dimension est cependant également applicable à des dynamiques qui ne sont pas spécifiquement spatiales. DeLanda (2006) affirme ainsi que la territorialisation peut par exemple consister dans le processus d'exclusion d'une certaine catégorie d'individus d'un groupe, ce qui renforce l'homogénéité entre les membres de cette organisation. De notre point de vue, la territorialisation exclut et homogénéise des groupes d'individus, mais aussi les déroulements possibles des actions et des relations au

sein d'un agencement. En d'autres termes, la territorialisation peut être définie comme un processus qui tend à homogénéiser la structure de l'espace des possibles et des marges d'action au sein de l'agencement. Par opposition, la déterritorialisation est un processus qui ouvre plus largement le cours possible des actions et des relations.

Cette seconde dimension nous autorise à conceptualiser les processus de stabilisation/consolidation (territorialisation) et de déstabilisation/rupture (déterritorialisation) de l'agencement. Dans ce qui suit, nous apportons un support empirique à cette approche de la triche.

L'AGENCEMENT DU MMORPG

Dans un article récent intitulé « The Assemblage of Play », Taylor (2009) explore certains des apports du concept d'agencement pour les *game studies*. Taylor ne fait pas directement référence à l'agencement de DeLanda, et souligne juste une faible parenté avec les travaux de Deleuze et Guattari (1987) et de Latour (2005). L'article de Taylor nous paraît intéressant, car il établit un lien entre la notion d'agencement et les MMORPG. Taylor présente les MMORPG comme des objets qui apparaissent particulièrement complexes en ce qu'ils résultent de l'imbrication d'un ensemble d'éléments distincts tels que des structures juridiques, des studios de développement, des joueurs, des technologies, et ainsi de suite. Taylor insiste plus particulièrement sur l'importance cruciale de ce qu'elle appelle « les relations réciproques » qui existent entre ces éléments et de ce qui résulte de ces influences réciproques. Elle affirme : « Dans l'espace de ces relations réciproques reposent les processus dynamiques de l'activité de jeu » (Taylor, 2009, p. 332). Pour Taylor, par conséquent, ce qu'est « jouer » résulte de l'agencement du MMORPG. Suite à notre présentation de la théorie de l'agencement selon DeLanda, nous pouvons certainement paraphraser Taylor en disant que « dans l'espace de ces relations réciproques repose le processus dynamique de la triche ».

On peut facilement dresser une esquisse du caractère composite des MMORPG et de la réciprocité des liens entre ses éléments variés qui sont identifiés par Taylor. Pour jouer à un MMORPG, un joueur doit d'abord acheter ou télécharger un logiciel client et l'installer sur un ordinateur. Lors du processus d'installation, il doit souscrire à différents documents juridiques tels le Contrat de Licence Utilisateur Final (CLUF) et les Conditions d'utilisation : le fait de souscrire à ces documents établit une relation juridique entre le joueur et

l'éditeur du jeu. Après l'installation, le joueur doit encore connecter son logiciel client au serveur du jeu et seulement alors, il peut commencer à jouer. Dans la plupart des cas, il aura également recours à Internet pour y chercher des guides, des solutions ou autres *paratextes* (Consalvo, 2007) relatifs au jeu. Il apparaît déjà là une série initiale de relations entre des éléments hétérogènes – joueurs, logiciel, licences – qui font partie de l'agencement des MMORPG.

Dans ce qui suit, nous attirons l'attention sur trois éléments de cet agencement dont le rôle est crucial pour la triche : l'architecture du jeu, le code et les documents juridiques. Nous décrirons l'articulation de ces éléments avec les pratiques des joueurs, les studios de développement et les entreprises qui fournissent des logiciels de triche.

Ce que nous entendons par « code » constitue une part importante de l'agencement du MMORPG. Le code comprend entre autres : le logiciel client du jeu, le programme du jeu qui est exécuté sur le serveur, et les logiciels antitriche, aussi bien que les logiciels qui sont utilisés par les tricheurs. Le code frauduleux[10] comprend les « bots » : des programmes informatiques qui opèrent via des routines d'intelligence artificielle pour automatiser certaines tâches du jeu, comme tuer et « looter » (ramasser le butin) les monstres. Les bots agissent comme des agents joueurs automates (Golle & Ducheneau, 2005 ; Joshi, 2008) dans ce qu'on appelle « jouer en AFK » (*Away From Keyboard*, loin du clavier) : le bot joue à la place du joueur humain. Les artéfacts textuels, tels que les articles scientifiques ou les brevets, peuvent pour leur part jouer un rôle essentiel dans la configuration de l'usage des technologies (voir Latour, 1987). Sur ce point, la documentation juridique des logiciels ne fait pas exception. Elle tient un rôle important dans la configuration des pratiques des utilisateurs et des développeurs de logiciels (Humphreys et al., 2005 ; de Paoli et al. 2008). Ces documents jouent également un rôle notable au sein de l'agencement du MMORPG. Le dernier élément crucial ici est l'architecture (cf. Castronova, 2005, chap. 3), c'est-à-dire la façon dont les ordinateurs impliqués dans le fonctionnement du jeu communiquent et sont reliés les uns aux autres (cf. Smed et al., 2002).

Ces éléments – le code, les documents juridiques et l'architecture – et leurs influences réciproques peuvent être décrits suivant les axes matériel/expressif et territorialisation/déterritorialisation de l'agencement. Ce faisant, nous concentrons notre attention sur la structure de l'espace des possibles qui est dessinée

10. *Cheating code* : instruments techniques (p. ex. des décompilateurs) et méthodes (p. ex. l'ingénierie inverse) compris.

par l'agencement et à partir de laquelle sont définis ce qui est virtuel (ce qui est possible en principe) et ce qui est actuel (ce qui est concrètement réalisé).

Les données mobilisées dans cet article proviennent de la combinaison d'une observation participante en cours dans le MMORPG Tibia (Atkinson & Hammersley, 1994), et d'analyses effectuées à partir du contenu du site et des forums officiels de Tibia et d'entreprises proposant des programmes de triche pour ce jeu[11]. La plupart des exemples qui sont sollicités ici concernent l'usage des bots dans Tibia, une pratique qui induit la manipulation illégale du code du jeu et de la communication entre machines. Nous pensons en effet que le botting est une pratique particulièrement révélatrice des dynamiques de l'agencement de la triche, car elle met en lumière la réciprocité des relations entre de nombreux éléments des MMORPG, dont le code du jeu et des programmes de triche ; les documents juridiques, leurs applications et infractions ; l'architecture du jeu et son éventuelle exploitation abusive. L'observation de la pratique du botting permet également de mettre au jour les actions et les stratégies de joueurs loyaux, de tricheurs, d'entreprises qui développent des jeux et de celles qui proposent des moyens de tricher.

Tibia a été choisi comme cas d'étude, car CipSoft (2009a), le développeur et éditeur de Tibia, a entrepris une campagne antitriche contre l'usage des bots depuis janvier 2009. Pour les besoins de l'analyse, nous avons concentré notre attention sur les posts des forums qui sont directement liés à la campagne antitriche de Tibia. Nous mobilisons également des données empiriques que nous avons recueillies lors d'une étude préliminaire sur la triche dans les MMORPG (conduite entre septembre et novembre 2008) et qui portent sur l'outil antitriche développé et édité en 2004 par Blizzard Entertainment (http://www.worldofwarcraft.com) et qui est utilisé pour *World of Warcraft* (WoW). Cette étude préliminaire nous a permis d'identifier des thématiques récurrentes dans les phénomènes de triche (p. ex. le rôle des outils antitriche) et de nous familiariser avec le vocabulaire technique et spécifique des MMORPG.

Dessiner l'architecture de la triche dans les MMORPG

Nous commencerons par décrire le rôle tenu par l'architecture du jeu, c'est-à-dire par la façon dont les machines qui sont impliquées par son fonctionne-

11. Forums officiels de Tibia : http://forum.tibia.com/forum/?subtopic=communityboards ; forums des sociétés de triche : http://www.blackdtools.com/forum/ et http://forums.tibiabot.com/

ment communiquent. L'architecture la plus communément utilisée dans les MMORPG est l'architecture client-serveur, qui est composée d'un serveur central auquel sont connectés plusieurs clients – les machines des joueurs (cf. figure 2). L'une des particularités de cette architecture est que la majorité du code du jeu est exécutée sur le serveur, et que le client n'en contrôle qu'une petite fraction. Dans cette configuration de la communication entre les machines, le client envoie une requête au serveur, cette requête est rejetée ou validée par le serveur, qui envoie le cas échéant la réponse à cette requête aux autres clients. Lorsque, par exemple, un personnage de Tibia comme Talah Teon (cf. figure 1) tue un monstre – ici un *slime*, cette action doit dans un premier temps être validée par le serveur. Le résultat de cette action – l'augmentation en niveau obtenue par Talah Teon – est ensuite communiqué par le serveur aux autres clients. Puisqu'il doit valider toutes les requêtes, le serveur peut aussi refuser certaines actions (p. ex. empêcher Talah Teon d'entrer dans la maison d'une guilde ennemie).

L'une des raisons pour lesquelles cette architecture est favorisée par la plupart des développeurs est qu'exécuter la plus grande partie du code sur le

Figure 1. (Capture d'écran de Tibia). Interface de jeu.
Un avatar (Talah Teon) engage un combat avec des monstres (« slimes »)

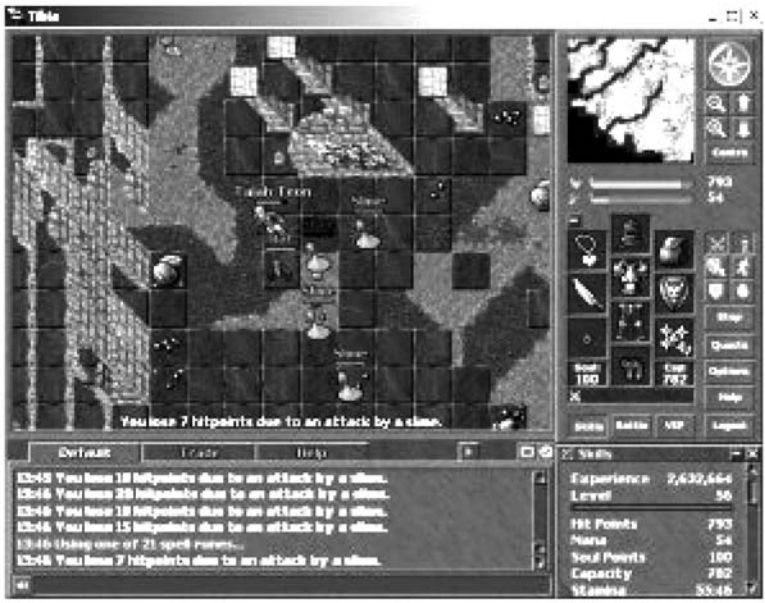
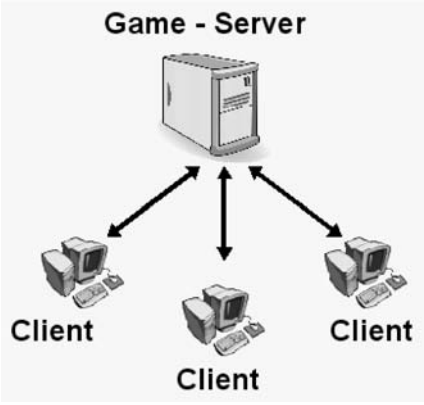


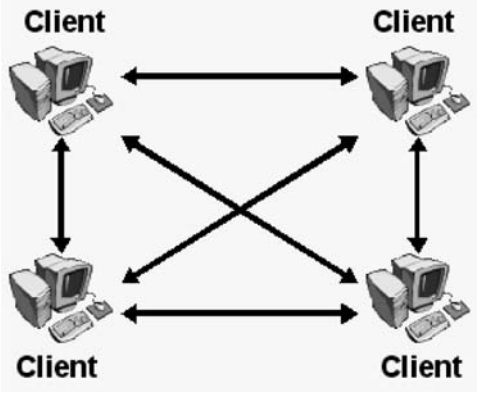
Figure 2. L'architecture client-serveur



serveur – dont celle dont dépendent les décisions les plus importantes du jeu, permet de garder un contrôle sur les activités des joueurs (Kabus et al., 2005). On considère que d'autres architectures disponibles, comme l'architecture peer-to-peer (cf. figure 3), dans laquelle l'information pertinente dépend des machines des autres joueurs (Barron, 2001) procurent un moindre contrôle sur les machines des joueurs.

Le choix de l'architecture client-serveur en tant que solution optimale en matière de sécurité nous permet de souligner la présence d'une dynamique virtuel/actuel. En effet, les développeurs disposent de nombreux modèles d'architectures pour gérer les MMORPG dont l'architecture client-serveur,

Figure 3. L'architecture Peer-to-Peer



l'architecture peer-to-peer, et une combinaison des deux. C'est cependant le premier modèle qui est utilisé dans la majorité des MMORPG, dont *World of Warcraft* et Tibia. Sur trois modèles (*a minima*) d'architecture disponibles, un seul est ici actualisé. Autrement dit, en adoptant pour Tibia une architecture client-serveur, CipSoft actualise un possible où l'architecture configure la pratique du jeu de manière à ce que pour que le joueur puisse jouer, le client de Tibia doive se connecter à l'un des serveurs de Tibia. De surcroît, la plupart des choix concernant le jeu (p. ex., valider la mort d'un monstre) sont réalisés sur les serveurs de CipSoft et sont ensuite communiqués aux autres clients.

En autorisant l'exercice d'une surveillance rapprochée de l'exécution du code du jeu, le choix d'une l'architecture client-serveur suggère aussi un effet de territorialisation par lequel les développeurs et éditeurs du jeu tentent de réduire la gamme des actions de triche possibles. Il est par exemple assez difficile pour les joueurs ou les tricheurs de modifier ou d'exploiter abusivement le code qui est stocké, exécuté et manipulé sur le serveur, alors qu'il est relativement aisé de le faire avec le code qui est stocké et exécuté sur le client. Cette observation vaut de manière générale : l'information et le code du jeu qui sont contrôlés et exécutés sur les machines des joueurs – dont les fichiers, la mémoire, les drivers, les services, etc. – peuvent en principe être l'objet de manipulation illégale (Pritchard, 2000).

L'architecture client-serveur possède donc une capacité de territorialisation spatiale qui consiste à exécuter de préférence code sur les machines de l'entreprise, plutôt que le déterritorialiser vers les machines des joueurs, dispersées géographiquement. On traduira l'idée que les accès, les ressources et la sécurité des données sont exclusivement contrôlés au niveau du serveur par la centralisation, en termes techniques.

La territorialisation spatiale de l'architecture – ou centralisation – ne peut cependant jamais être totale, et une partie de l'information reste toujours stockée ou manipulée par les clients. En effet, pour des raisons de performance notamment, tous les états[12] du jeu ne peuvent être hébergés sur le serveur. Hoglund et McGraw (2008, p. 142) en détaillant l'organisation de la structure des données[13] d'un personnage de MMORPG, affirment, par exemple, que si

12. La notion d'état renvoie aux valeurs contenues dans la mémoire, dans les registres ou tout autre composant physique de l'ordinateur qui est affecté par l'exécution d'un programme.
13. La structure des données est la façon dont sont organisées et stockées les données informatisées.

ces données sont bien en général stockées sur le serveur du jeu, c'est parfois le programme client qui contrôle directement leurs valeurs. Or si le client contrôle certaines valeurs de la structure de données d'un personnage, alors un programmeur expert pourra aisément manipuler ces valeurs pour obtenir un avantage déloyal – par exemple, améliorer une des compétences de ce personnage, en manipulant les valeurs qui y sont liées. Dans les jeux en ligne de stratégie en temps réel, par exemple, il est parfois possible de manipuler frauduleusement l'information du client qui définit les « zones non explorées » de la carte du jeu (Pritchard, 2000), et donc de conférer un avantage déloyal à un joueur en lui permettant connaître les positions des unités ennemies.

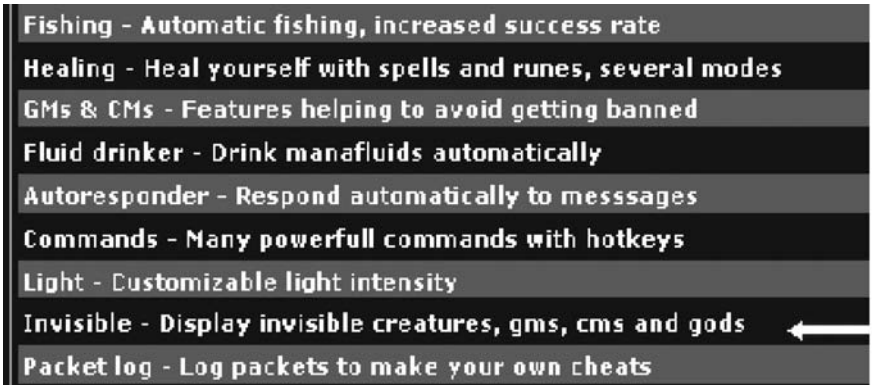
Cet extrait d'une communication officielle de CipSoft est un bon exemple de centralisation : « Ne pensez-vous pas qu'une créature invisible devrait être invisible pour tous les joueurs ? Nous le pensons. C'est pourquoi nous allons rendre plus efficace l'invisibilité des monstres, ce qui affectera principalement les joueurs qui trichent pour cibler ces créatures. (...) Notre client ne contiendra plus aucune information concernant les monstres invisibles. Il sera désormais impossible de pointer des runes missiles sur les coordonnées d'une créature invisible. »

Ce message a été publié par CipSoft (2009b) parallèlement à une mise à jour du logiciel client. CipSoft a manifestement ici décidé de déplacer du client vers le serveur les informations qui concernent les créatures invisibles du jeu. Les créatures invisibles sont des monstres du jeu ayant la capacité de tirer sur des personnages joueurs sans révéler leur position. Il est donc difficile pour le joueur de localiser l'origine de ces attaques. Avant la mise à jour, les informations concernant la localisation de ces créatures étaient directement administrées par le client, ce qui de l'aveu même de CipSoft rendait cette information susceptible d'être manipulée pour tricher.

Manifestement, nous avons affaire ici à un effort de territorialisation spatiale qui vise à restreindre les opportunités de triche en déplaçant l'information sur les « monstres invisibles » des clients de jeu déterritorialisés vers les serveurs de jeu centralisés.

La décision de territorialiser les monstres invisibles a été prise par CipSoft afin de contrecarrer certains types d'exploitations abusives commises par les joueurs au travers de l'usage de bots. Certains bots de triche connus, comme BlackDProxy (cf. figure 4), TibiabotNG et Elfbot permettent en effet facilement d'identifier (« d'afficher ») et donc de tuer les monstres invisibles.

Figure 4 – Quelques fonctionnalités de BlackDProxy, y compris l'affichage des monstres invisibles



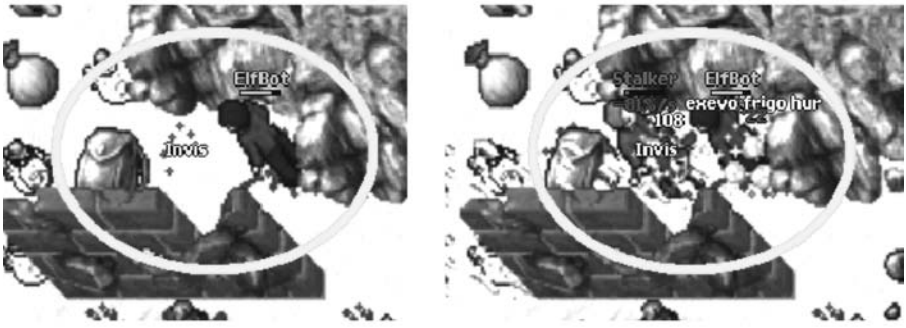
La territorialisation de ces monstres vers le serveur a entraîné une déterritorialisation — une déstabilisation – chez les bots de la fonctionnalité d'affichage des monstres invisibles. Cela a déclenché un contre-processus de territorialisation chez les tricheurs de Tibia, qui ont tenté de contourner l'obstacle en restabilisant cette fonctionnalité des bots. Les joueurs qui utilisaient Elfbot ont, par exemple, mis en place un contournement qui permet au bot de localiser les monstres même si l'information n'est plus manipulée par le client : certains sorts du personnage sont utilisés pour repérer la position du monstre afin que le bot puisse le cibler. La figure 5 montre à gauche comment le sort « Vague de glace » est utilisé pour la détection d'une créature invisible et, à droite, le meurtre du monstre identifié (« Stalker ») par Elfbot.

Appliquer les règles et garder les utilisateurs sous contrôle

Lorsque les joueurs installent le logiciel client sur leur ordinateur, ils doivent souscrire à un certain nombre de textes, dont le CLUF, les Conditions d'utilisation, et souvent d'autres encore, tels que des règles du jeu ou des chartes de confidentialité (Castronova, 2005 ; Kane, 2009)[14]. Les documents juridiques reflètent l'architecture des jeux : le logiciel client dépend du CLUF, tandis que le logiciel qui tourne sur les serveurs est protégé par les Conditions d'utilisation. Pour jouer au jeu, les joueurs doivent accepter le contenu de ces

14. Lien vers les documents juridiques de Tibia : http://www.tibia.com/support/?subtopic=legaldocuments, et de WoW : http://eu.blizzard.com/fr-fr/company/legal/

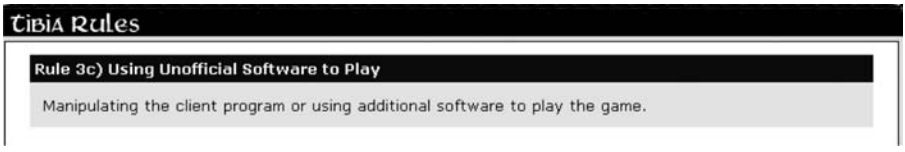
Figure 5 – Contournement de la détection des monstres invisibles. Adapté de : http://forums.tibiabot.com/showthread.php?t=76436



documents. En ce sens, les licences logicielles participent de la structure de l'espace des possibles, possibles dont l'actualisation peut passer par des éléments du code, comme les outils antitriche.

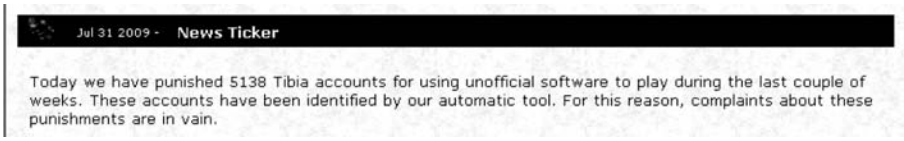
L'analyse des documents juridiques est primordiale pour comprendre comment le phénomène de triche émerge de l'agencement du MMORPG. Ces textes ont des implications diverses pour les joueurs et les entreprises de jeu vidéo, dont le renoncement par les joueurs à certains de leurs droits (Castronova, 2005 ; Kane, 2009). Souvent, les licences et autres documents juridiques définissent les termes de la prévention ou de la régulation d'une série de pratiques frauduleuses, dont l'exploitation abusive de bugs, l'usage d'applications tierces ou l'ingénierie inverse du client. La règle numéro 3 de Tibia, intitulé « Triche » interdit, par exemple, l'exploitation abusive des bug, le *hacking*, etc. La règle 3c, « Jouer avec un logiciel non officiel » énonce pour sa part l'interdiction pour les joueurs de manipuler le programme du client, et d'utiliser un logiciel tiers pour jouer.

Figure 6 – La règle 3c) « Using Unofficial Software to Play » de Tibia qui interdit l'usage d'un logiciel tiers pour jouer : « Manipulating the client or using additional software to play the game. »



Les textes juridiques ne contiennent pas seulement des règles qui délimitent virtuellement le périmètre d'action des joueurs. Elles comportent également des règles qui définissent les sanctions qui seront reçues par les joueurs s'il y a violation du règlement. Concernant Tibia, il y est précisé que CipSoft peut exclure – temporairement ou définitivement – les joueurs du jeu à partir du moment où ceux-ci ont enfreint ses règles (CipSoft *Extended Service Agreement*, 2009c). Encore une fois, il faut souligner le caractère virtuel de ces régulations, qui composent un espace de possibles qui sont actualisés seulement sous certaines conditions. Courant 2009 CipSoft a, par exemple, procédé dans le cadre de sa campagne antitriche, à des suspensions massives de joueurs (cf. figure 7)[15]. La plupart de ces suspensions correspondaient à la violation de la règle 3c, référant à l'usage de bots. Ces suspensions illustrent l'actualisation à la fois des règles de Tibia – qui interdisent l'usage de logiciels tiers – et de l'*Extended Service Agreement* – qui définit la sanction applicable en cas d'infraction.

Figure 7 – Actualisation des règles de Tibia[16]. Annonce de la suspension sans recours possible de 5138 comptes joueurs



Pour souligner encore une fois la dialectique virtuel/actuel des documents juridiques, on peut évoquer le fait que le joueur « expressif » (i.e. le statut sémiotique de joueur qui est défini par la licence) diverge du joueur « matériel », fait lui de chair et d'os. La règle 3c de Tibia définit, par exemple, le joueur comme une personne qui ne manipule pas le client du jeu et n'utilise pas de logiciel tiers pour joueur. Pourtant, nous avons déjà mentionné l'existence des bots, qui constitue de toute évidence une violation de cette règle. L'analyse des forums des entreprises qui vendent des bots pour Tibia démontre aussi que de nombreux joueurs ont recours à l'usage de bots. Cet usage est enfin tout à fait connu dans la communauté des joueurs de Tibia et constitue un sujet de discussion récurrent sur les forums officiels[17].

---

15. Dix suspensions massives jusqu'à présent, avec l'exclusion (temporaire) de près de 50 000 comptes de jeu.
16. Extrait de : http://www.tibia.com/news/?subtopic=newsarchive&id=1048&fbegind=12&fbeginm=4&fbeginy=2009&fendd=12&fendm=10&fendy=2009&flist=11111111.
17. Par exemple, http://forum.tibia.com/forum/?action=thread&threadid=1978162.

L'une des solutions pour appliquer le CLUFs et les Conditions d'utilisation est la création et le déploiement d'outils antitriche [18]. Ces dispositifs logiciels appliquent automatiquement les termes des textes juridiques. Ils fonctionnent donc comme les formes matérielles d'éléments plus expressifs (i.e. les documents juridiques). Consalvo (2007, chap. 6) distingue précisément trois types d'outils : (1) les outils qui visent à empêcher la triche – par exemple en cryptant la communication client-serveur ; (2) les outils qui visent à mettre un terme à la triche – par exemple en déconnectant le tricheur une fois qu'il est détecté ; et enfin (3) les outils qui visent à détecter l'usage des logiciels tiers (tels que des bots) qui interfèrent avec le logiciel client, détection qui peut aboutir à la suspension des tricheurs.

Les logiciels antitriche ont également une capacité de territorialisation : ils facilitent la prévention comme la sanction de pratiques de triche telles que l'usage de bots et dans une certaine mesure, ils permettent aux entreprises de jeu vidéo de stabiliser l'équilibre et l'équité des conditions de jeu. À l'occasion de la campagne antitriche de Tibia, CipSoft a mis en place un nouvel outil antitriche, il est néanmoins difficile de l'étudier, car son fonctionnement est tenu secret par l'entreprise. Afin de mieux appréhender le potentiel de territorialisation des outils antitriche, nous proposons donc une brève analyse du rôle de l'outil antitriche de Blizzard connu sous le nom de « the Warden » (« le Gardien ») (Blizzard, 2005). Le fonctionnement de cet outil antitriche est en effet assez bien documenté. Lorsque le joueur connecte son client au serveur de *World of Warcraft*, le Warden est téléchargé du serveur vers la machine client de l'utilisateur. Un Warden est téléchargé et mis en route toutes les 15 secondes environ. Le Warden est composé de petites portions de code qui sont réassemblées dynamiquement lors de chaque chargement et les portions de code qui sont assemblées diffèrent légèrement à chaque fois, ce qui signifie que chaque Warden est unique. Il est donc difficile de concevoir un code frauduleux qui puisse échapper à son contrôle : même si un tricheur « capture » un Warden et crée un programme pour le contrer, ce programme ne sera pas efficace, car le Warden qui sera chargé par la suite sera différent de celui qui a été capturé (Hoglund & McGraw, 2008). Ici, nous pouvons voir comment les outils antitriche participent de l'agencement de la triche en territorialisant le code frauduleux – en réduisant son efficacité et donc en augmentant l'homogénéité.

18. De nombreux outils antitriche sont mobilisés par les entreprises de jeu vidéo. Un exemple répandu est « Punkbuster ». Voir http://www.evenbalance.com/.

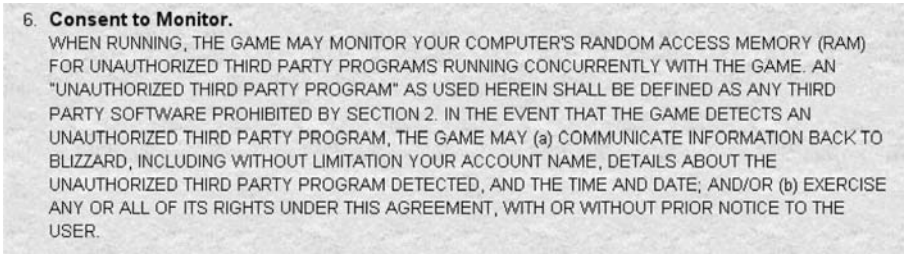
Les outils antitriche sont par ailleurs des objets controversés de l'agencement du MMORPG : le caractère particulièrement intrusif du Warden lui confère une signification plus profonde que celle de neutralisation des pratiques de triche. En scannant la RAM[19] de la machine du joueur et par le biais d'autres actions intrusives, comme l'envoi de captures d'écran vers les serveurs du jeu, le Warden agit en effet comme un logiciel-espion (*spyware*, cf. Tardiman, 2005). Le Warden parcourt le code qui est exécuté sur la machine des joueurs et le compare avec un répertoire des codes frauduleux connus pour *World of Warcraft* qui est mis à jour sur les serveurs de Blizzard. Si le code qui est exécuté sur la machine du joueur est répertorié, son usage est considéré comme une infraction et il peut déclencher une sanction de suspension voire de suppression du compte du joueur. L'association du Warden et du répertoire de code frauduleux maintenu par Blizzard actualise de manière concrète la frontière entre le code qui est détecté comme frauduleux et celui qui ne l'est pas. Il est intéressant de noter qu'ici, le Warden produit un double effet de territorialisation-déterritorialisation. En effet, le contrôle des infractions possibles – définies par la documentation légale – n'est pas exercé sur les serveurs de l'entreprise dans un premier temps, mais il est déterritorialisé sur les machines des joueurs. Le Warden surveille en permanence ce qui se passe sur les machines des joueurs et opère dans un deuxième temps seulement une territorialisation, en rapportant l'information sur les serveurs.

Nous avons dit comment un outil tel que le Warden pouvait parcourir les machines des joueurs à la recherche de code frauduleux. Le contrôle qui est exercé par le Warden sur les machines des joueurs est rendu possible par le fait que le joueur a souscrit aux documents juridiques et à une clause en particulier qui autorise cette surveillance (« *Consent to Monitor* »)[20]. Il y a une relation matérielle/expressive entre le Warden et cet accord pour la surveillance. Le Warden exerce matériellement une surveillance et d'autres formes de contrôle – constituant une version digitale du *panoptique* foucaldien ou de ce que Baman nomme le *panspectron*, alors que la clause par laquelle joueur consent à ce contrôle est le terme juridique qui définit une discipline de la surveillance, en conférant à l'entreprise le droit d'exercer un contrôle sur les machines des joueurs. Il s'agit par ailleurs d'une illustration de la façon

19. *Random Access Memory*, mémoire vive, inscriptible temporairement, de l'ordinateur.
20. Les CLUFs d'autres MMORPG comportent des clauses similaires. C'est le cas de *Runescape* (Règle 7), de *Warhammer* (CLUF, point 2G), de *Age of Conan* (CLUF, point 5). Pour Tibia, la politique de confidentialité autorise l'usage d'outils antitriche : http://www.tibia.com/support/?subtopic=legaldocuments&page=privacy.

dont le CLUF d'un jeu impose aux joueurs de se défaire de certains de leurs droits.

Figure 8 – Le consentement à la surveillance.
Extrait de http://www.worldofwarcraft.com/legal/eula.html 21


6. **Consent to Monitor.**
WHEN RUNNING, THE GAME MAY MONITOR YOUR COMPUTER'S RANDOM ACCESS MEMORY (RAM) FOR UNAUTHORIZED THIRD PARTY PROGRAMS RUNNING CONCURRENTLY WITH THE GAME. AN "UNAUTHORIZED THIRD PARTY PROGRAM" AS USED HEREIN SHALL BE DEFINED AS ANY THIRD PARTY SOFTWARE PROHIBITED BY SECTION 2. IN THE EVENT THAT THE GAME DETECTS AN UNAUTHORIZED THIRD PARTY PROGRAM, THE GAME MAY (a) COMMUNICATE INFORMATION BACK TO BLIZZARD, INCLUDING WITHOUT LIMITATION YOUR ACCOUNT NAME, DETAILS ABOUT THE UNAUTHORIZED THIRD PARTY PROGRAM DETECTED, AND THE TIME AND DATE; AND/OR (b) EXERCISE ANY OR ALL OF ITS RIGHTS UNDER THIS AGREEMENT, WITH OR WITHOUT PRIOR NOTICE TO THE USER.

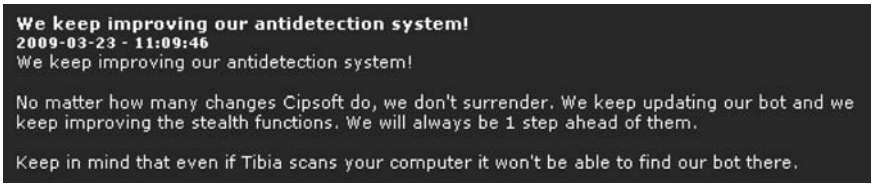
Une illustration supplémentaire du rôle qui est tenu par les outils antitriche nous est fournie par Tibia. Comme évoqué précédemment, un outil antitriche a été mis en place début 2009 lors de la campagne antitriche de CipSoft dans l'optique de neutraliser l'usage des bots et des logiciels tiers.

Les MMORPG sont souvent affectés par l'existence d'entreprises tierces qui produisent et vendent des bots pour automatiser les actions de jeu. Un exemple célèbre est le programme « Glider » qui est utilisé pour World of Warcraft (se référer pour plus de détails à Consalvo, 2009, pp. 412-413). Deux « sociétés de triche », nommées respectivement BlackDTools (produisant BlackDProxy) et NGSoft (produisant TibiaBot NG et Elbot), créent des bots pour Tibia. Du point de vue de ces sociétés, les outils antitriche ont produit un effet de déterritorialisation : l'outil a déstabilisé les pratiques de programmation existantes ainsi que les relations commerciales qui existaient entre ces sociétés et les tricheurs (de Paoli & Kerr, 2010). Avant l'introduction d'un outil antitriche, les relations entre les sociétés de triche et leurs clients étaient relativement stables : l'usage de bots était très rarement repéré par les maîtres de jeu (*game masters*) de Tibia et restait généralement impuni par CipSoft. Le marché des bots était alors florissant. En rendant les bots détectables, l'outil antitriche a brisé cette stabilité. Les sociétés de triche, à la recherche d'un effet de territorialisation qui pourrait stabiliser à nouveau ces

21. NdT. Dans la version française du jeu, cette clause se trouve dans la section « XVI. Informations particulières » des Conditions d'utilisation de *World of Warcraft*, disponibles sur http://eu.blizzard.com/fr-fr/company/legal/wow_tou.html.

relations (cf. figure 9), tentent depuis de concevoir les bots indétectables que leur demandent leurs clients.

Figure 9 – Concevoir des bots indétectables



Le potentiel expressif des mesures antitriche

Pour limiter les pratiques de triche, les développeurs peuvent recourir à plusieurs stratégies. Nous avons évoqué les outils antitriche et leur capacité matérielle à performer le potentiel expressif des documents juridiques, en particulier en ce qui concerne les bots. Nous avons également présenté le potentiel de territorialisation de ces outils en tant que moyen de restreindre le spectre des pratiques de triche possibles. Un effet de territorialisation peut aussi être exercé par la conception d'éléments dans les mécanismes de jeu (*gameplay*) visant à restreindre la triche (Consalvo, 2007). Des « Monstres Antibot Intelligents »[22] — *Antibot Intelligent Monsters* (AIM) – ont, par exemple, été introduits dans Tibia pour neutraliser le jeu en AFK et l'usage des bots. Ces AIM ressemblent à des monstres ordinaires et portent le même nom qu'eux, mais ils infligent en fait beaucoup plus de dommages au joueur que des monstres courants. En outre, ils se soignent très rapidement, ce qui les rend presque impossibles à tuer. Le rôle tenu par les AIM a un caractère expressif, dans la mesure où ils sont issus de l'exécution du code du serveur de jeu. Ces monstres apparaissent ainsi comme le produit expressif – non fonctionnel – du code matériel – fonctionnel – qui les génère. Il faut donc prendre en considération le fait que les mesures antitriche ne s'exercent pas nécessairement comme les outils antitriche de manière matérielle.

Lorsque des joueurs humains de Tibia rencontrent ces AIM, le mieux pour eux est de fuir, car ils infligent des dommages très importants et tuent facilement les personnages joueurs, même puissants. Un personnage automatisé

22. Voir http://forums.tibiabot.com/showthread.php?t=101002.

avec un joueur en AFK a plus de risques d'être éliminé par les AIM. En effet, les personnages qui sont joués par des bots attaquent automatiquement les AIMs et ne cherchent pas à s'enfuir, car ils ne sont pas en mesure de différencier ceux-ci de monstres ordinaires. Dans la majorité des cas, les AIM tuent ainsi le personnage qui est contrôlé par un bot. L'introduction des AIM a conduit à une innovation chez les tricheurs de Tibia qui ont développé des contournements : de petits scripts qui permettent aux bots de reconnaître des AIM. Une solution simple au problème soulevé par les AIM est en effet d'écrire un script qui entraîne le bot à ignorer un monstre à partir du moment où le combat dure plus qu'un temps déterminé – disons par exemple 15 secondes : SI (« Combat.temps > 15 Secondes » & « Monstre = vivant ») ALORS (« Désengager le combat » & « Fuir »). Un autre contournement tire avantage du fait que les AIM se déplacent en général à une vitesse différente des monstres ordinaires. Un simple script permet alors de détecter cette différence de vitesse et apprend aux bots à ignorer les AIM. Le code présente dans ce cas à la fois une capacité de territorialisation et de déterritorialisation. En autorisant les bots à ignorer les AIM, il contribue à stabiliser les activités de triche, mais dans le même temps, il rend inefficaces les AIM en tant que mesures antitriche.

VERS UNE NOUVELLE APPROCHE DE LA TRICHE : LE CONTRE-JEU COMME IMBROGLIO

Nous sommes d'avis que, si le concept d'agencement se révèle utile pour approcher la triche, il peut aussi contribuer conceptuellement plus largement à notre compréhension de ce qu'est le contre-jeu. Le concept d'agencement peut être mobilisé pour étudier ce qui émerge de la réciprocité des relations qui sont établies entre les composantes d'un monde virtuel à travers le temps et, par conséquent, il peut contribuer à un renouvellement de la perception de ce qui peut constituer le contre-jeu. Afin d'apprécier justement les modalités de cette contribution, nous devons cependant préciser certains éléments et souligner ce en quoi le concept de contre-jeu est spécifique. Le concept de contre-jeu peut être abusivement interprété comme une forme de résistance de la part des joueurs et comme une subversion des modes de jeu, ce qui doit être modéré si nous souhaitons travailler cette notion avec celle d'agencement. En effet, en argumentant pour une étude des relations réciproques entre éléments de l'agencement du MMORPG, nous avons dans cet article rejeté ce genre de qualifications *a priori* des phénomènes, fondées uniquement sur les actions et motivations des joueurs.

Plusieurs études se sont penchées sur les modes de jeu déviant de ceux prescrits par la conception et le script du jeu. L'un des concepts qui est déployé pour saisir ces phénomènes est le « jeu transgressif », défini comme l'acte par lequel un joueur exprime une rébellion vis-à-vis des règles du jeu (Aarseth, 2007). Plusieurs exemples de styles de jeu subversifs et d'exploitation des failles du jeu insistent pour leur part sur la façon dont les joueurs altèrent la figure du « joueur idéal » imaginé et scripté par les concepteurs du jeu. Suivant une logique similaire, Atkins (2003, pp. 49-50) évoque le plaisir qui peut être éprouvé dans la conduite d'un jeu transgressif et subversif. Ces travaux portent donc leur attention sur les actions plus ou moins populaires qui constituent un détournement des règles du jeu et des bonnes manières de jouer telles qu'elles ont été conçues par les concepteurs. Sundén (2007, p. 2) porte plus loin le concept de « jeu transgressif » en avançant l'idée que jouer transgressivement revient à jouer de manière innovante, et que, bien que le jeu situe un joueur idéal, les joueurs sont tout autant situés par une culture plus large du jeu. Son travail porte sur la manière dont les joueurs gay et lesbiens développent des modes de jeu « queer » qui vont à l'encontre des régulations et de la conception des jeux en ligne. Ce concept de jeu transgressif reste selon nous trop axé sur les actions individuelles des joueurs et peine à saisir le dynamisme relationnel de l'agencement du MMORPG.

Une autre approche, portée par Kücklich (2009), tente de tenir compte du caractère hétéroclite des espaces du jeu, qui est à la fois constitué d'espaces réglés et d'espaces non réglés. Selon Kücklich, il convient de considérer non seulement les antagonismes qui prennent place au sein du jeu, mais aussi les contextes politiques, sociaux et culturels dans lesquels ces antagonismes s'inscrivent. Il propose de considérer la triche comme une pratique « dé-ludique » qui certes, ramène au premier plan les dispositifs machiniques des systèmes de jeux vidéo, mais implique plus que le joueur et la technologie, et nous entraîne dans un espace de jeu « dé-territorialisé ». Cette déterritorialisation affirme et met au jour l'existence de liens entre le réel et le virtuel. À la différence des auteurs précédents, il suggère donc que la triche est moins une tentative d'affirmation d'une identité qu'une tentative d'opposition à des contraintes et de refonte intégrale de la topologie d'un jeu. (Kücklich, 2009, p. 165). Comme telle, elle peut être considérée à des échelles variables en tant qu'acte politique. L'idée que l'utilisateur et la machine entretiennent une relation réciproque modelée par un contexte plus large que celui des règles du jeu est assez proche de notre perspective, même si cette théorie n'a pas été éprouvée empiriquement.

Ces travaux mettent en avant la volonté qu'ont les chercheurs de saisir la lutte qui est engagée entre le véritable joueur du jeu et le message qui est porté par le jeu au travers de ses règles et du script d'un joueur idéal ou implicite. Bien que cette relation puisse être perçue comme une lutte de pouvoir, un conflit, la négociation des règles fait fondamentalement partie du plaisir qui est éprouvé dans les jeux (Marshall, 2002). Sans aller jusqu'à surestimer la maîtrise des joueurs sur le jeu ou leur capacité à s'opposer aux règles, il paraît évident que l'agencement du MMORPG n'est pas statique : ses éléments sont continuellement remodelés en fonction des relations contingentes et réciproques qu'ils entretiennent. Ce qu'est « jouer » (Taylor, 2009), comme ce qu'est « tricher » découle de l'agencement du MMORPG. Nous pensons que les pratiques que nous avons étudiées sont plus que transgressives au sens où elles ont des conséquences sur la topologie du jeu dans son ensemble, et bien au-delà du seul espace immédiat de jeu. En effet, le jeu avec ou dans l'espace du jeu est fait par les joueurs, les éditeurs de jeu et les sociétés tierces. Par conséquent, nous pensons qu'une approche du contre-jeu doit dépasser la description des actes individuels et peut-être marginaux des joueurs, et inclure d'autres éléments tels que l'architecture du jeu, les documents juridiques, le code, et d'autres acteurs, dont les entreprises de jeu vidéo et la technologie.

Nous soutenons l'idée que la triche émerge des dynamiques qui sont générées par « l'entrecroisement des propriétés du réel et du virtuel, qui œuvrent à mobiliser une suite de sujets, d'objets et de choses en vue de fins variées »[23]. Or il s'agit précisément de ce que la notion d'agencement nous permet de développer, soit (1) une approche non essentialiste et (2) une analyse de ce qui émerge – le produit – de l'agencement du MMORPG.

À ce point, il est manifeste que nous ne pouvons uniquement envisager la triche dans les MMORPG comme ce qui procure un avantage déloyal aux tricheurs. Des éléments tels que « l'architecture », le « code» sous différentes formes – dont le code du jeu, les outils antitriche et les programmes de bot – et les « documents juridiques » ne procurent pas en eux-mêmes un avantage déloyal aux tricheurs. Néanmoins, de nombreuses composantes des phénomènes de triche découlent de la réciprocité de leurs relations et de leur capacité à faire jouer simultanément leurs pouvoirs expressifs et matériels, territoralisant

23. NdT. Cette définition renvoie au contenu de l'appel à propositions pour le dossier spécial « Counterplay » de la revue *Fibreculture*. Cet appel est consultable sur http://www.digra.org/news_old/archive/2009/08/04/cfp-counterplay-gaming-cheating-and-control-special-issue-of-fibreculture-journal.

et deterritorialisant. Les rapports virtuels/actuels qui existent entre les règles du jeu, leur déploiement et leur violation par les tricheurs émergent des relations qui existent réciproquement entre le code, les documents juridiques et l'architecture. La surveillance qui est exercée par les entreprises de jeu vidéo sur les machines des joueurs dépend également des relations réciproques qui sont établies entre les outils antitriche, les documents juridiques et l'architecture. Les Monstres antibot (AIM) en tant que mesure antitriche relèvent également des liens entre la matérialité du code exécuté et la capacité expressive des AIM à faire partie des mécanismes de jeu (*gameplay*).

Nous avons ouvert cet article en nous demandant comment il serait possible de définir la triche dans les MMORPG. Nous avons démontré les limites des définitions courantes de ce phénomène – et particulièrement de celles qui sont induites par une approche essentialiste. Nous restons cependant pour le moment dépourvus d'une définition concrète qui pourrait être mobilisée dans de futurs travaux empiriques ou théoriques. Il nous paraît donc important de conclure ce texte en tentant de fournir une nouvelle définition de la triche dans les MMORPG et les jeux en ligne qui s'appuie sur le concept d'agencement.

Lorsque nous parlons de triche, nous utilisons le mot « triche » (*cheating*) dans le sens qu'il prend dans la langue anglaise. Le dictionnaire Oxford anglais fournit plusieurs définitions de la triche[24], dont la suivante : « agir avec malhonnêteté ou de manière déloyale dans le but d'obtenir un avantage »[25]. Cette définition est identique à celle qui est mobilisée de façon essentialiste dans la majorité de la littérature sur la triche. Dans d'autres langues cependant, le terme de triche possède des significations sensiblement différentes et qui peuvent s'avérer utiles pour nous. La traduction italienne de la triche : *barare* signifie agir malhonnêtement afin d'obtenir un avantage déloyal, en particulier dans le contexte d'activités ludiques – comme celui d'un jeu de cartes. Mais en italien, on peut également traduire « tricher » par *imbrogliare* ou « triche » par *imbroglio*. Le mot *imbroglio* existe aussi en anglais, il est défini par le dictionnaire Oxford comme « un état d'enchevêtrement et de grande confusion ; une situation compliquée ou difficile (politiquement, dramatiquement) ; un malentendu confondant, un différend ou une embrouille ». Cette définition ne retient toutefois que certains points de la définition du terme en italien, qui a un sens plus ambivalent. Il désigne à la fois un entremêlement confus

24. Dont : tromper une personne (comme une femme qui trompe son mari), ou s'approprier le bien d'autrui…
25. http://www.askoxford.com/concise_oed/cheat?view=uk.

de choses et une ruse, soit le fait de piéger quelqu'un dans le but d'obtenir quelque chose de manière indue. Plus exactement, c'est grâce à l'imbroglio comme enchevêtrement, confusion et manipulation d'éléments divers que la ruse peut fonctionner. Nous pensons que le terme d'imbroglio peut constituer le socle de la nouvelle définition de la triche fondée sur le concept d'agencement que nous recherchons.

La qualification de la triche par le terme d'imbroglio trouve appui dans le travail du sociologue Bruno Latour qui conceptualise les relations entre ce qu'il appelle les humains et les non-humains et qui rejette les approches essentialistes fondées sur des perspectives duales. Latour (1999, p. 204) parle d'« imbroglios sociotechniques » pour décrire, en lieu d'un dualisme sujet-objet cartésien, le réseau sans coutures des humains et non-humains. L'usage fait par Latour du terme imbroglio, bien qu'il ait une portée plus générale, est très proche du nôtre. Suivant Latour, un imbroglio sociotechnique est tout d'abord non-essentialiste, car il rejette les propriétés essentielles de sujet ou d'objet. Il est ensuite fondé sur des relations réciproques (acteurs réseau) et sur l'enchevêtrement hétérogène d'humains et de non-humains. C'est le cas du laboratoire, qui est composé à la fois de scientifiques et d'instruments techniques. Les produits de ces imbroglios sociotechniques sont pour Latour (1987, pp. 128-129) des machinations – des ruses selon nos termes, c'est-à-dire des technologies opérantes ou des preuves indiscutables.

Nous proposons donc le terme imbroglio comme nouveau point de départ pour les études sur la triche dans les MMORPG, car il favorise l'approche de la triche comme un agencement. Le cas de Tibia est riche en imbroglios. Les AIM constituent, par exemple, une forme d'imbroglio où des relations s'établissent entre l'exécution du code, les monstres qui semblent normaux, et les limites des routines de l'intelligence artificielle des bots. Les bots de Tibia, incapables de reconnaître l'imbroglio sont victimes de la ruse. Un autre exemple est fourni par les bots eux-mêmes dont l'existence et l'usage entrelace étroitement le code informatique – celui des bots mais aussi du jeu – et les documents juridiques, de sorte que l'agent joueur automate agisse comme un joueur humain. Il y a là production d'un imbroglio, puisque les autres joueurs – mais aussi les outils antitriche et les maîtres du jeu (*game masters*) – doivent croire qu'un humain joue le personnage. Si l'impression générale est qu'il s'agit d'un humain et non d'un bot, il n'y a pas violation des documents juridique.

Pour conclure, approcher les MMORPG comme des assemblages, et définir la triche comme un imbroglio constitue une alternative utile pour réfléchir ce

phénomène et contribuer à la construction de la notion de contre-jeu. Le fait que notre mobilisation de l'imbroglio soit limitée à un domaine particulier – celui de la triche dans les MMORPG – comparativement à l'usage qu'en fait Latour, n'amoindrit pas notre intuition initiale. Au contraire, il rend l'usage de ce concept plus pertinent encore comme point de départ de travaux empiriques et théoriques. Nous souhaitons en effet aborder la triche comme imbroglio en prenant appui sur les approches qui adoptent une perspective non essentialiste similaire. Nous entendons par là des cadres conceptuels tels que la théorie de l'agencement (DeLanda, 2002, 2006), la théorie de l'acteur réseau (Latour, 1987, 2005) et la critique de l'information (Lash, 2002). Ainsi, « la triche comme imbroglio » apparaît bien comme un nouveau point de départ pour explorer les dynamiques relationnelles de la triche dans les MMORPG et ce qu'elles produisent.

REMERCIEMENTS

Les auteurs souhaitent remercier l'*Irish Higher Education Authority* pour son soutien sur le programme PRTLI 4, ainsi que ses collaborateurs sur le projet « Serving Society: Future Communications Networks and Services » (2008-2010), sans oublier les deux relecteurs anonymes de la revue *Fibreculture* pour leurs remarques pertinentes.

RÉFÉRENCES

AARSETH, E. (2007). “I Fought the Law: Transgressive Play and The Implied Player”, in *Situated Play, Proceedings of the DiGRA 2007*. Tokyo, Japon, 2007. Disponible sur http://www.digra.org/dl/db/07313.03489.pdf.

ATKINS, B. (2003). *More than a game. The computer game as fictional form*. Manchester: Manchester University Press.

ATKINSON, P. & HAMMERSLEY, M. (1994). “Ethnography and participant observation”, in Denzin, Norman & Lincoln (Eds.), *Handbook of Qualitative Research.* Sage. Thousand Oaks, Canada, pp. 248-261.

BARDZELL et al. (2007). “Virtual Worlds and Fraud: Approaching Cybersecurity in Massively Multiplayer Games”, in *Situated Play, Proceedings of the DiGRA 2007*. Tokyo, Japon. Disponible sur http://www.digra.org/dl/db/07311.42219.pdf.

BARRON, T. (2001). *Multiplayer game programming*. Roseville: Prima Publishing.

BELL, M. V. (2008). “Toward a Definition of Virtual Worlds”, *Journal of Virtual Worlds Research*, *1*(1).

BLIZZARD ENTERTAINMENT (2004). *World of Warcraft*. http://www.worldofwarcraft.com.

(2005). “A Statement on Our Hack-Scanning Process”, disponible sur http://web.archive.org/web/20051211091852/http://forums.worldofwarcraft.com/thread.aspx?fn=blizzard-archive&t=33&p=1&tmp=1.

BRAMAN, S. (2005). *Change of State: Information, Policy, and Power.* Cambridge: MIT Press.

BROOKE, P. J. et al. (2004). “Playing the game: cheating, loopholes, and virtual identity”, in *ACM SIGCAS Computers and Society*, 34, 2. Disponible sur http://portal.acm.org/citation.cfm?id=1052791.1052794.

CASTRONOVA, E. (2005). *Synthetic worlds: The Business and Pleasure of Gaming*. Chicago: Chicago University Press.

CIPSOFT (1997). *Tibia.* http://www.tibia.com (Site web).

(2009a). “Where Will Cheaters Go From Here?”, 2009a, disponible sur http://www.tibia.com/news/?subtopic=latestnews&id=910.

(2009b). “Second Patch Teaser: Stamina, Experience Counter and More”, disponible sur http://www.tibia.com/news/?subtopic=newsarchive&id=945&fbegind=29&fbeginm=2&fbeginy=2009&fendd=29&fendm=3&fendy=2009&flist=11111111.

(2009c). “Extended Service Agreement”, disponible sur http://www.tibia.com/support/?subtopic=legaldocuments&page=extendedagreement.

(2009d). "Tibia Rules", disponible sur http://www.tibia.com/support/?subtopic=tibiarules.

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

(2009). "There is No Magic Circle", *Games and Culture*, *4* (4) 408-417.

DELANDA M. (2002). *Intensive Science and Virtual Philosophy.* London: Continnuum.

(2006). *A New Philosophy of Society: Assemblage Theory and Social Complexity.* London: Continnuum.

DELEUZE, G. & GUATTARI, F. (1987). *A Thousand Plateaus.* London: Athlone.

(1988). *Foucault.* London: Athlone.

DE PAOLI, S. & KERR, A. (2010). "'We Will Always Be One Step Ahead of Them': A Case Study on the Economy of Cheating in MMORPGs", *Journal of Virtual Worlds Research*, *4* (2). Disponible sur https://journals.tdl.org/jvwr/article/view/865.

DE PAOLI, S. et al. (2008), "*Free and open source licenses in community life*", *First-Monday*, *13* (10). Disponible sur http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/view/2064/2030.

DURKHEIM, É. (1951). *A Study in Sociology*. Glencoe: The Free Press (1re edition, 1897).

ENISA (2008). "Virtual worlds, real money security and privacy in massively-multiplayer online games and social and corporate virtual worlds". Disponible sur : http://www.enisa.europa.eu/pages/02_01_press_2008_11_20_online_gaming.html.

FOO, C. & KOIVISTO, E. M. (2004). "Defining grief play in MMORPGs: player and developer perceptions", in *Proceedings of the ACM SIGCHI international Conference on Advances in Computer Entertainment Technology.* New York, pp. 245-250.

FOUCAULT, M. (1977). *Discipline and Punish: The Birth of the Prison*. London: Penguin.

GOLLE, P. & DUCHENEAUT, N. (2005). "Preventing bots from playing online games", *Compt. Entertain*, *3* (3). Disponible sur http://portal.acm.org/ft_gateway.cfm?id=1077255&type=pdf&coll=GUIDE&dl=GUIDE&CFID=58484236&CFTOKEN=67331407.

HARMAN, G. (2008). "DeLanda's ontology: assemblage and realism", *Continental Philosophy Review*, *41* (3) 367-383.

HOGLUND, G. & MCGRAW, G. (2008). *Exploiting Online Games: Cheating Massively Distributed Systems*. Addison-Wesley Professional.

HUMPHREYS, S. et al. (2004). « Fan based production for computer games: User led innovation, the 'drift of value' and the negotiation of intellectual property rights (IPRs) », *Media International Australia*, n° 114. pp. 16-29.

JOSHI, R. (2008). “Cheating and Virtual Crimes in Massively Multiplayer Online Games”, *Technical Report RHUL-MA-2008-06*. Department of Mathematics, Royal Holloway, University of London, Disponible sur http://www.ma.rhul.ac.uk/static/techrep/2008/RHUL-MA-2008-06.pdf.

KANE, S. F. (2009). “Virtual Judgment: Legal Implications of Online Gaming”, *IEEE Security & Privacy*, *7* (3) 23-28.

KERR, A. (2006). *The business and culture of digital games: gamework/gamplay*. London: Sage.

KABUS, P. et al. (2005). “Addressing cheating in distributed MMOGs”, in *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support For Games*. New York, NY: ACM, pp. 1-6.

KÜCKLICH, J. (2007). “Homo Deludens: Cheating as a methodological tool in digital games research”, *Convergence*, *13* (4) 355-367.

(2009). “A Techno-Semiotic Approach to Cheating in Computer Games: Or How I Learned How to Stop Worrying and Love the Machine”, *Games and Culture*, *4* (2) 158-169.

LATOUR, B. (1987). *Science in Action, How to Follow Scientists and Engineers through Society* Cambridge Mass.: Harvard University Press.

(1999). *Pandora’s Hope*. London: Harvard University Press.

(2005). *Reassembling the Social: An Introduction to Actor-Network Theory*. Oxford: Oxford University Press.

LASH, S. (2002). *Critique of Information*. London: Sage.

MARSHALL, D. P. (2002). “The New Intertextual Commodity”, in Harries, D. (Ed.), *The New Media Book*. London: BFI, pp. 69-81.

PARKER J. (2007). “Cheating by Video Game Participants”, *Loading… 1* (1).

PARSONS, T. (1951). *The Social System*. Glencoe: Free Press.

PRITCHARD, M. (2000). “How to Hurt the Hackers: The Scoop on Internet Cheating and How You Can Combat It”, *Gamasutra* (24 juillet). Disponible sur http://www.gamasutra.com/features/20000724/ pritchard_pfv.htm.

SALEN, K. & ZIMMERMAN, E. (2003). *Rules of Play: Game design Fundamentals.* Cambridge Mass.: The MIT Press.

SMED, J. et al. (2002). “Aspects of networking in multiplayer computer games”, *The Electronic Library*, *20* (2) 87-97.

SMITH, J. H. (2004). “Playing Dirty: Understanding Conflicts in Multiplayer Games”, *5th Annual Conference of The Association of Internet Researchers*, The University of Sussex, 19 septembre. Disponible sur http://jonassmith.dk/weblog/uploads/playing_dirty.pdf.

SUNDEN, J. (2009). "Play as Transgression: An Ethnographic Approach to Queer Game Cultures", in *Breaking New Ground, Proceedings of the DiGRA 2009*, Brunel University, UK. Disponible sur http://www.digra.org/dl/db/09287.40551.pdf.

TAYLOR, T. L. (2006). *Play Between Worlds: Exploring Online Game Culture*. Cambridge, Mass.: The MIT Press.

(2009). "The Assemblage of Play", *Games and Culture*, *4* (4) 331-339.

TERDIMAN, D. (2005). "Game players say Blizzard Invades Privacy", in *CNET News.* Disponible sur http://news.cnet.com/Game-players-say-Blizzard-invades-privacy/2100-1043_3-5830718.html.

YAN, J. Y. & CHOI, H. J. (2002). "Security Issues in Online Games", *The Electronic Library*, *20* (2) 125-133.

YAN, J. Y. & RANDELL, B. (2005). "A systematic classification of cheating in online games", in *Proceedings of 4th ACM SIGCOMM Workshop on Network and System Support For Games* New York, NY: ACM.

WEBB, S. D. & SOH, S. (2007). "Cheating in networked computer games: a review", in *Proceedings of the 2nd international conference onDigital interactive media in entertainment and arts*. New York, NY: AMC, pp. 105-122.