Les espaces des conflits numériques

Samuel Rufat, Hovig ter Minassian

Les espaces des conflits numériques

Samuel Rufat, Université de Cergy-Pontoise
Hovig Ter Minassian, Université de Tours

« Watch a 12-years-old take evasive action and score multiple hits while playing *Space Invaders*, and you will appreciate the skills of tomorrow's pilot »
Ronald Reagan, discours au Disney World en Floride, 8 mars 1983

« This isn't a video game. It's a war. A real war »
Colin Powell, interviewé sur *Fox News* le 24 mars 2003, quatre jours après l'invasion en Irak

Depuis la Seconde Guerre mondiale, les outils numériques, informatiques et de communication ont pris une place prépondérante dans les conflits*. Désormais, les moyens de pression des différents acteurs s'expriment aussi bien sur le champ de bataille que dans le cyberespace*. Le cyberespace peut être l'enjeu d'un conflit portant sur un marché ou sur des informations stratégiques, l'espace-support du conflit dans le cas des cyberattaques*, ou bien l'outil essentiel de la maitrise de champs de bataille éloignés.

Pourtant, il est difficile de parler de « cyberconflit* ». Il n'y a pas de conflit virtuel : quand un antagonisme a émergé, le conflit est réel. Il est précédé par différentes phases de tension qui sont tout autant réelles. Par ailleurs, tous les passages à l'acte (piratage* informatique) et tous les moyens de pression (attaques de serveurs*) ne sont pas uniquement déployés sur les réseaux informatiques et de communication. Il s'agit plutôt d'une numérisation des conflits, par le recours croissant depuis le début de la Guerre Froide à la puissance de calcul, à la performance des réseaux de communication et à la numérisation de l'information. Historiquement, ces outils numériques ont d'abord été développés pour faire la guerre. Ils ont fait émerger de nouveaux moyens de confrontation ou de régulation, mais ils visent à perturber l'équilibre des systèmes « réels ».

En fait, c'est plutôt la simulation des conflits qui leur confère un caractère virtuel. Le conflit repose sur une tension actualisée, alors que le virtuel se situe dans l'univers des possibles, avant leur actualisation par les choix des acteurs et leurs interactions avec le contexte [Lévy, 1998]. Lorsqu'un conflit émerge d'une opposition ou d'une rivalité, la tension ne peut être résolue que par l'élimination, physique ou symbolique, d'un des acteurs du conflit (en cas de guerre par exemple) ou de l'objet du conflit (par exemple un projet d'aménagement contesté). En revanche, la simulation permet de conserver le caractère virtuel d'une tension et d'explorer les conséquences possibles des différents choix qui s'offrent aux acteurs. C'était l'objet des *wargames*, et avant eux des jeux de stratégie plus abstraits comme les échecs ou le go. Depuis l'Antiquité, des jeux simulent les conflits dans presque toutes les cultures [Kline, 2003]. Ces jeux et ces simulations ont suivi la même numérisation que les conflits, en accompagnant l'émergence des jeux vidéo. C'est donc du côté des jeux vidéo, comme dernier avatar de cette numérisation des conflits, qu'il faut chercher les conflits virtuels et les cyberconflits.

I Les réseaux informatiques : nouveaux territoires de conflits

1 Les cyberattaques accompagnent les conflits militaires

L'importance prise par la numérisation des conflits peut faire de l'information et des réseaux de communication un enjeu. C'est pourquoi le cyberespace s'est transformé en champ de bataille lors de conflits récents. Les « cyberattaques » sont de nouveaux types d'offensives qui viennent s'ajouter à des opérations militaires ou de renseignement plus classiques. Elles ne se

substituent cependant pas aux opérations militaires. Bien qu'elles se déroulent dans le cyberespace, elles ne sont pas déterritorialisées : elles ont lieu en majeure partie aux États-Unis, en Russie, ou encore en Chine [Ventre, 2010] et elles ciblent des États, des entreprises, des réseaux ou des serveurs informatiques qui ont une localisation précise. La géographie des cyberattaques exprime ainsi les rapports de force géopolitiques contemporains.

Dans la nuit du 7 au 8 août 2008, la Russie a déclenché une opération militaire contre la Géorgie en envahissant l'Ossétie du Sud. Dès le 20 juillet 2008, soit deux semaines avant l'invasion, le cyberespace géorgien avait été attaqué à l'aide de plusieurs réseaux d'ordinateurs piratés (*botnet*) qui l'avaient saturé de requêtes jusqu'à rendre les serveurs inutilisables (attaque* par déni de service distribué ou *DDoS*). Le site web du président géorgien Mikheil Saakashvili a été attaqué en premier (les photos du président ont été remplacées par celles d'Adolf Hitler), puis les sites de l'administration et des médias, empêchant le gouvernement géorgien de communiquer jusqu'à la fin des opérations terrestres. Enfin, le 7 août, soit la veille de l'offensive terrestre, l'ensemble du trafic géorgien a été redirigé vers le serveur russe Bryansk.ru. L'ampleur, la coordination et le calendrier de cette attaque ont fait dire qu'elle avait été planifiée depuis Moscou, même si aucune preuve n'a pu en être apportée [Markoff, 2008].

D'autant plus qu'il existe un précédent : la cyberattaque de l'Estonie entre avril et mai 2007, suite au déboulonnage de la statue du soldat de bronze, érigée en 1947 à la mémoire des soldats soviétiques de la Seconde Guerre Mondiale dans le centre ville de Tallinn. Cette cyberattaque a été à l'origine de la création par l'OTAN* à Tallinn du Centre de cyberdéfense en coopération (*Cooperative* Cyber Defence Centre of Excellence*, CCDCOE) le 14 mai 2008. En mai 2010, l'OTAN a mené des « cybermanœuvres » à Tallinn, le *Baltic Cyber Shield* (bouclier informatique balte), reproduisant une cyberattaque comme celles de 2007 et 2008 et essayant d'envisager le pire, que des pirates informatiques parviennent à déclencher le lancement d'un missile à partir de l'Internet.

2 La cyberguérilla, un conflit asymétrique

Les cyberattaques ne concernent pas seulement les États, mais aussi les entreprises, les organisations et les particuliers, dans le cadre de la compétition économique ou de tensions politiques. Ainsi, la société Google a révélé en janvier 2010 que ses serveurs en Chine avaient été attaqués et qu'un important volume de données y avait été dérobé en décembre 2009. Google a accusé Pékin et a menacé de ne plus censurer les données sur son portail google.cn, comme la société s'y était engagée en 2006 auprès des autorités pour pouvoir accéder au marché chinois [Markoff, 2010].

Il est difficile de déterminer l'origine d'une cyberattaque parce que l'agresseur s'abrite souvent derrière un réseau d'ordinateurs qu'il a piraté. De plus, elle repose sur une asymétrie : il faut beaucoup de ressources pour s'en prémunir, mais un ordinateur ancien avec une connexion par modem sont suffisants pour pénétrer un serveur ou le saturer. En 2010, le conflit entre Wikileaks* et les autorités américaines a conduit à une « cyberguérilla ». Après la révélation de 200 000 documents confidentiels, dont des documents classés « secret défense » sur les guerres en Irak et en Afghanistan, le 28 novembre 2010, les transferts bancaires à destination de Wikileaks ont été bloqués par les sociétés *Visa*, *MasterCard* et *PayPal*. En représailles, des sympathisants ont lancé l'opération *Payback* en décembre 2010 : une série d'attaques par déni de service (*DoS*) contre les sites de ces sociétés et contre la banque suisse *PostFinance* qui avait gelé un compte du fondateur de WikiLeaks, Julian Assange.

En fait, l'asymétrie propre aux cyberattaques pourrait faire se déporter de nombreux conflits, de natures très différentes, dans le cyberespace. Les cyberattaques sont attractives et

accessibles en raison d'un anonymat qui peut être parfois préservé et du peu de moyens nécessaires. On peut même louer les services d'organisations criminelles sur l'Internet, à partir de 50 euros la cible. Il s'agit d'une nouvelle façon pour des acteurs aux moyens limités de faire changer un conflit d'échelle, qu'il s'agisse de représailles, de faire pression sur des acteurs plus puissants ou de dérober de l'information. Ce changement d'échelle découle de la propriété des réseaux : la mise hors service d'un serveur entrave les flux sur un territoire étendu et parfois sans relation avec l'emplacement des serveurs. Pour éviter cette situation, les serveurs sont très interconnectés, ce qui permet de rediriger les flux, mais favorise aussi la propagation de programmes informatiques malveillants bien au-delà de leurs cibles initiales.

II Informatique et complexe militaro-industriel

1 L'informatisation des conflits

Les débuts de l'informatique sont liés à la mobilisation des mathématiciens pendant la Deuxième Guerre Mondiale. Les travaux d'Alan Turing (1912-1954) ont conduit à la construction en 1943 de la « Bombe » (calculateur électromécanique) puis en 1944 de Colossus (calculateur à tubes à vide) près de Londres, pour casser les codes secrets Enigma[1]. Les travaux de John von Neumann (1903-1957) ont conduit en 1944 à la construction de l'EDVAC (*Electronic* Discrete Variable Automatic Computer*) à l'Université de Pennsylvanie pour répondre aux besoins du Laboratoire en recherche balistique de l'armée américaine. Jusque dans les années 1970, le Ministère de la Défense des États-Unis reste le premier acquéreur matériel informatique [Fortin, 2007]. Le DARPA (*Defense* Advanced Research Projects Agency*) est aussi à l'origine du cyberespace, avec la mise en réseau des ordinateurs des centres de recherche financés par les crédits militaires : l'ARPANET*, au début des années 1960. Cette numérisation progressive permet une mise à distance, territoriale et symbolique, de la violence des conflits.

Ainsi, pendant la Guerre du Vietnam, l'armée américaine avait installé près de 20 000 capteurs électroniques pour surveiller les 250 km de front (opération *Igloo White*). À distance, au *White Infiltration Surveillance Center* situé en Thaïlande, les plus puissants processeurs informatiques de l'époque (IBM 360/65) traitaient l'information en temps réel et affichaient les données sur des écrans avec des cartes. Ces informations étaient transmises aux forces aériennes pour qu'elles interviennent dès qu'une incursion nord-vietnamienne était détectée. En imposant une médiation numérique entre le soldat et sa cible, l'utilisation d'outils informatiques dans les conflits contemporains déshumanise la guerre [Halter, 2006]. Elle la rend à la fois plus supportable et plus aseptisée, parce que le soldat n'a plus de prise directe sur la conséquence de ses actes.

Plus récemment, le conflit en Afghanistan est mis à distance par le recours à des drones qui sont pilotés depuis des centres de commande très éloignés du champ de bataille. Pour les pilotes qui utilisent ce type d'outils, la cible est déshumanisée, réduite à quelques pixels sur un écran d'ordinateur. La mise à distance est double : à la fois métrique (le pilote se trouve dans un pays en paix à l'autre bout du monde) et cognitive (le dispositif technique imposant une médiation entre le soldat qui prend la décision de tirer et la perception des conséquences de son geste [Dubey, 2009]).

2 La simulation des conflits

La simulation des conflits s'est longtemps appuyée sur des jeux qui servaient d'entrainement. En 1664, Christopher Weikhmann s'est inspiré des échecs pour proposer de former

[1] Machine qui servait à coder ou décoder des messages secrets, et qui fut notamment utilisée pendant la seconde guerre mondiale par l'Allemagne nazie.

l'aristocratie à la guerre avec un jeu de plateau, le *Koenigspiel*. Par la suite, ce type de jeu s'est développé en parallèle de la militarisation des sociétés européennes au cours du 19ème siècle. En 1824, l'officier prussien Helmut von Moltke publie les règles du jeu intitulé *Instructions pour la représentation de manœuvres tactiques sous l'apparence d'un jeu de guerre* ou *Kriegspiel* (Annart 2008). Même chez les pacifistes, le jeu de guerre était mobilisé, cette fois-ci pour dénoncer la barbarie, comme le jeu de stratégie *Little Wars* du romancier Herbert George Wells [Halter, 2006].

L'émergence des jeux vidéo s'inscrit dans cette filiation entre jeu et guerre. Historiquement, elle est liée à celle de l'informatique, à la structuration du complexe* militaro-industriel aux États-Unis et à la numérisation des conflits au cours de la Guerre Froide. Le premier jeu informatique, un jeu de morpion sur 9 cases (*XOX*), a été programmé sur le successeur de l'EDVAC*, l'EDSAC* (*Electronic Delay Storage Automatic Calculator*), construit en 1949 à l'Université de Cambridge pour faire des calculs balistiques. En 1958, William Higinbotham, ancien de l'équipe du projet Manhattan, a inventé le premier jeu vidéo, *Tennis for Two*, pour donner une image plaisante du laboratoire de physique atomique de Brookhaven. En 1962, Steve Russell a créé le jeu *Spacewar!* en profitant du temps libre sur les calculateurs du Massachussetts Institute of Technology (MIT), quand ils ne servaient pas à simuler des vols acrobatiques ou des apocalypses nucléaires. C'est avec ces crédits militaires qu'a été créé le premier jeu vidéo en réseau (*MazeWar*, 1973) au centre de recherche d'Ames de la NASA. Ce jeu a été interdit dès 1975 par le Ministère de la Défense américain, parce que les équipes de recherche jouant les unes contre les autres consommaient plus de la moitié de la bande passante de l'ARPANET au lieu de faire des calculs balistiques. Ces premiers « hackers » ont avancé que les investissements nécessaires au développement de l'informatique n'étaient possibles que grâce à l'armée américaine, et que ces financements les laissaient libres, parce que les militaires ne comprenaient pas leurs travaux et qu'ils n'attendaient pas de résultat à court terme. Toutefois, les militaires n'ont pas tardé à se réapproprier les jeux vidéo pour leurs besoins de simulation et de formation [Halter, 2006].

En 1980, les représentants du TRADOC* (*US Army's Training and Doctrine Command*) ont demandé à la société de jeux vidéo *Atari* de transformer son nouveau jeu *Battlezone* en simulateur d'entraînement (*Army Battlezone*). En 2002, l'armée américaine a financé le jeu *America's Army*, développé en collaboration avec des sociétés de conception de jeux vidéo (Ubisoft, Secret Level). Téléchargeable gratuitement en ligne, ce jeu a permis à l'armée de redorer son image, de faciliter le recrutement de jeunes joueurs/soldats et de stimuler leur entrainement. En 2003, l'ICT (*Institute for Creative Technologies*) de l'armée américaine a passé une commande à des concepteurs de jeux (THQ, Pandemic Studios) et des sociétés d'effets spéciaux (Sony Imageworks) pour la réalisation d'un jeu vidéo, *Full Spectrum Warrior*, destiné à servir de simulateur d'entraînement sur console de jeu.

L'informatisation de la simulation des conflits a stimulé l'émergence de l'industrie du jeu vidéo, mais l'interpénétration de ces deux univers brouille à dessein les limites entre guerre, jeu et leurs représentations. En Irak, l'armée américaine encourage les soldats à passer leur temps libre à joueur à des jeux de tir ou d'entrainement, qui reconstituent de plus en plus fidèlement le contexte de leurs missions [Halter, 2006].

III La guerre est-elle devenue un jeu ?

De par leurs origines, les jeux vidéo mettent en scène des guerres. Ils peuvent dès lors être considérés comme des « artefacts* culturels » et montrer la manière dont se transmettent les représentations et les valeurs d'une époque [Ter Minassian & Rufat, 2008]. Tout jeu vidéo repose sur du conflit : le joueur ne peut avancer que par élimination d'un obstacle, sous peine

d'être éliminé lui-même. Selon les jeux, l'obstacle peut prendre la forme d'un monstre, d'adversaires, d'un piège ou d'une énigme. Le conflit relève de la logique interne du jeu, mais aussi de sa logique externe, il est souvent l'occasion de la mise en scène, plus ou moins réaliste, d'un conflit ou d'une guerre.

Une autre raison de la prévalence de la violence et de la guerre dans les jeux vidéo découle de logiques commerciales. Au début des années 1990, Sega a essayé de détrôner la compagnie leader Nintendo en infantilisant les jeux de son concurrent, par exemple en montrant que son jeu *Mortal Kombat* était bien plus violent que le *Street Fighter* de Nintendo, dans une campagne publicitaire de 45 millions de dollars lancée en 1992. Il en a découlé une « course à la testostérone » [Kline, 2003] qui a débouché sur la multiplication de jeux violents et de jeux de guerres, toujours plus réalistes et sanglants. La « masculinité militarisée » [Kline, 2003] des jeux vidéo vise à cibler le public le plus rentable, les jeunes adolescents de sexe masculin, tout en faisant l'économie d'avoir à renouveler les scénarios ou les mécanismes de ces jeux, pour lesquels ont été mobilisés les informaticiens et les stratèges mis au chômage par la fin de la Guerre Froide [Halter, 2006].

La géographie des conflits dans les jeux vidéo a évolué en lien avec leur contexte de production et avec l'actualité. Les premiers jeux vidéo situent plutôt leur action dans des univers « hors du monde » ou sidéraux (*Spacewar !* 1962, *Pong* en 1972 ou *Space Invaders* en 1978), en lien avec la course aux étoiles de la Guerre Froide. Dans les années 1980 et 1990, ils s'ancrent dans des contextes historiques mais la Guerre Froide reste la référence, comme dans la série de jeux de stratégie *Command & Conquer: Red Alert* (1996-2008). L'autre contexte mobilisé est la Seconde Guerre Mondiale, lui aussi utilisé pour les simulations financées par le complexe industrialo-militaire américain, de la série des jeux de tir subjectif *Wolfenstein* (1981-2009) jusqu'à *Medal of Honor* (initiée en 1999) ou *Call of Duty* (initiée en 2003).

Balance of Power (1985) proposait au joueur d'incarner le camp américain ou le camp soviétique au cours de la Guerre Froide. La suite de ce jeu, sortie en 2009, *Balance of Power: 21th Century*, a été réalisée par le même concepteur, Chris Crawford. Le jeu se passe désormais après le 11 septembre 2001 et le joueur ne peut incarner que le président des États-Unis. On assiste à un basculement dans la géographie des conflits mis en scène par les jeux depuis 2001. Désormais, l'ennemi à abattre n'est plus le rouge de la Guerre Froide, mais le terroriste, et en particulier le terroriste islamique [Fortin, 2007]. Les deux séries *Medal of Honor* et *Call of Duty* sont ainsi passé des terrains de la Seconde Guerre Mondiale et de la guerre Groide, au Proche et au Moyen-Orient, avec une mise en scène du contre-terrorisme.

À l'inverse, on peut relever l'émergence parallèle d'une production vidéoludique anti-américaine ou anti-israélienne. Dans *The Night of Bush Capturing* (2006), développé par le *Global Islamic Media Front*, le joueur participe à la capture du président américain. Dans *UnderAsh* (2001), créé par une société syrienne, le joueur incarne Ahmed, un jeune Palestinien durant la première Intifada. La mise en scène des conflits contemporains exprime tout le potentiel de communication des jeux vidéo. Ils peuvent également servir à l'expression de discours pacifistes, à l'exemple du *September 12th: a Toy World* (2003), développé par Gonzalo Frasca, qui met en scène l'invasion irakienne pour mieux la dénoncer.

La cartographie des jeux vidéo de guerre exprime bien certaines logiques conflictuelles du monde contemporain, en les simplifiant parfois à l'extrême. Ces jeux donnent à lire les représentations et idéologies d'un monde en guerre. Mais l'invasion des médias par les conflits est bien plus générale, car la violence « fait vendre ». La numérisation des conflits permet une mise à distance territoriale et symbolique ou cognitive, d'autant plus que cette

percolation de la simulation de conflits dans les médias et dans les jeux accrédite l'idée de conflits virtuels, aux conséquences évanescentes. Mais le passage à l'acte de la tension au conflit s'inscrit toujours dans un territoire et ses conséquences sont « réelles ». En fait, le virtuel n'est que du côté de la simulation et des jeux vidéo [Rufat & Ter Minassian, 2011]. Finalement, le stade ultime de la numérisation des conflits, le cyberconflit qui ne se déroule *que* dans le cyberespace, ce sont les jeux vidéo massivement multi-joueurs.

Références

Annart J., « L'histoire du wargame », *Les cahiers du jeu vidéo*, 2008, n° 1.

Dubey G., intervention dans le cadre du séminaire « Jeux vidéo et travail », Laboratoire junior Jeux vidéo : pratiques, contenus, discours, ENS de Lyon, 16 décembre 2009.

Fortin T., « Guerre à la portée de tous », *Le monde diplomatique*, juillet 2007.

Halter E., *From Sun Tzu to Xbox. War and Video Games*, Thunder's Mouth Press, New York, 2006.

Kline S, Dyer-Witheford N., De Peuter G., *Digital Play. The Interaction of Technology, Culture, and Marketing*, McGill-Queen's University Press, 2003.

Lévy P., *Qu'est ce que le virtuel ?*, La Découverte, Paris, 1998.

Markoff J., « Before the Gunfire, Cyberattacks », *The New York Times*, August 12, 2008.

Markoff J., « Cyberattack on Google Said to Hit Password System », *The New York Times*, April 19, 2010.

Rufat S., Ter Minassian H. (dir.), *Les jeux vidéo comme objet de recherche*, Questions Théoriques, Lecture>Play, Paris, 2011.

Ter Minassian H., Rufat S., « Et si les jeux vidéo servaient à comprendre la géographie ? », *Cybergéo*, n° 418, 2008.

Ventre D. (dir), *Cyberguerre et guerre de l'information. Stratégies, règles, enjeux*, Hermès Science-Lavoisier, Paris, 2010.

GLOSSAIRE

ARPANET : réseau informatique créé en 1969 pour relier tous les ordinateurs et les serveurs des différents centres de recherche, laboratoires ou universitaires travaillant avec le DARPA.

Artefact : « Fait par l'art, c'est-à-dire par le travail humain » (Brunet R., Ferras R., Théry H., *Les mots de la géographie*, Reclus-La documentation française, Montpellier, Paris, 1993).

Attaque par déni de service distribué (DDoS) : cyberattaque visant à rendre un serveur ou un ordinateur inopérant en lui adressant un maximum de données inutiles via le réseau auquel il est connecté.

Complexe militaro-industriel : désigne « un acteur extrêmement puissant dans l'économie et le territoire de certains pays, au point d'y assurer une partie notable de la production de l'espace (…). Le complexe militaro-industriel se signale d'un côté par les installations de l'armée ; d'un autre par les ensembles industriels de l'armement et de ses dérivés (…), enfin par le poids qu'il applique sur les décisions et les comportements de l'État et de son appareil » (Brunet R., Ferras R., Théry H., *Les mots de la géographie*, Reclus-La documentation française, Montpellier, Paris, 1993).

***Cooperative Cyber Defence Centre of Excellence (CCDCOE)* :** organisation militaire rattachée à l'OTAN et créé en 2008 pour promouvoir et améliorer la défense des réseaux informatiques des pays membres de l'OTAN contre tous types de cyberattaques. Le centre est situé à Tallinn, en Estonie.

Cyberattaque : acte d'agression ayant lieu dans le cyberespace, le plus souvent au moyen de logiciels malveillants visant à voler des informations, corrompre des données, ou prendre contrôle d'un ordinateur distant.

Cyberconflit : désigne un conflit qui se déroulerait dans le cyberespace. En réalité, il n'existe pas de cyberconflit. Toute cyberattaque ayant lieu dans le cyberespace vise à la déstabilisation de systèmes « réels ».

Cyberespace : "A consensual hallucination experienced daily by billions of legitimate operators (…) Lines of light ranged in the nonspace of the mind, clusters and constellations of data". William GIBSON, 1984, *Neuromancer*, New York, Ace Books, p. 67.
On désigne communément par cyberspace l'ensemble des réseaux informatiques (comme Internet) qui permettent l'échange d'informations et de données.

***Defense Advanced Research Projects Agency (DARPA)* :** centre de recherche du département américain de la Défense, dont le principal objectif est de maintenir la supérieur technologique des États-Unis dans le domaine militaire. L'agence a été créée en 1958, après le lancement par l'Union Soviétique du satellite *Sputnik*.

Electronic Delay Storage Automatic Calculator (EDSAC) : un des tous premiers ordinateurs électroniques, construit en 1949 pour les besoins de l'université de Cambridge (RU).

***Electronic Discrete Variable Automatic Computer (EDVAC)* :** un des tous premiers ordinateurs électroniques, construit en 1949 pour répondre aux besoins du laboratoire de recherche en balistique de l'armée américaine.

***US Army's Training and Doctrine Command (TRADOC)*:** organisation dépendante de l'armée américaine, créée en 1973 pour améliorer la formation des troupes américaines, ce qui inclut l'entraînement au maniement des armes et des véhicules, la simulation de situations de combats ou encore l'assimilation de la doctrine militaire.

Piratage informatique : utilisation illégale et le plus souvent à des fins malveillantes d'un ordinateur.

Serveur (informatique) : désigne un ordinateur dont la principale tâche est de rend service aux ordinateurs et logiciels qui s'y connectent à travers un réseau informatique. Ce service peut consister à stocker des fichiers, transférer le courrier électronique, héberger un site Web, etc.