# Politiques du hacking : enquête sur les ruses numériques

Benjamin Loveluck, Jean-Vincent Holeindre

Quaderni

Communication, technologies, pouvoir

103 | Printemps 2021
Les ruses du *hacking*
Dossier

# Politiques du *hacking* : enquête sur les ruses numériques

BENJAMIN LOVELUCK ET JEAN-VINCENT HOLEINDRE

p. 9-24
https://doi.org/10.4000/quaderni.1970

## *Texte intégral*

> « *Les hackers sont des collectionneurs de ruses pour supprimer et contourner la normalisation de l'usage inscrite dans l'objet* »
> Nicolas Auray, EHESS, Paris, 2000, p. 15.

1 Dans sa plus simple expression, le *hacking* informatique peut se résumer à une solution ingénieuse apportée à un problème technique ou à la découverte de fonctionnalités imprévues. Toutefois, définir plus précisément le *hacking* est délicat, tant les pratiques qui s'y rapportent sont diverses, et peuvent même paraître contradictoires. Celles-ci vont de la programmation et de l'électronique à la sécurité informatique et l'administration réseau ; du codage de logiciels libres à l'accès aux biens culturels, sous la bannière parfois revendiquée de la « piraterie » ; de l'intrusion purement « exploratoire » dans des systèmes d'information au vol d'identifiants bancaires ou à la création de « rançongiciels » (*ransomware*). Un *hack* peut être de nature technique, mais aussi reposer sur la capacité à se faire passer pour quelqu'un d'autre lors d'une interaction afin de collecter des informations (*social engineering*). Certains hackers sont des bâtisseurs tandis que d'autres exploitent les failles (*exploits*) pour leur intérêt personnel ; une partie s'active aux marges du système de production de l'information et des mécanismes de contrôle qui l'accompagnent, alors que d'autres embrassent le capitalisme par projet et la course à l'innovation dont ils deviennent parfois la pointe avancée. Des hackers se regroupent en communautés très visibles et s'organisent en collectifs, tandis que d'autres travaillent seuls ou presque et avec une visibilité restreinte.

2 À cette diversité de pratiques répond une grande variété de rapports au politique.

Les formes d'engagement peuvent être explicites : c'est le cas par exemple du *hacking* dit « citoyen » ou *civic hacking* qui ambitionne de faciliter et d'accroître la transparence des institutions, d'encourager la participation démocratique, ou tout simplement d'apporter des solutions à des problèmes d'intérêt général (Crabtree 2007 ; Powell 2016 ; Schrock 2016 ; Ermoshina 2018). C'est vrai également du *hacktivisme* militant conçu comme une intervention tactique voire une « guerre informationnelle » dans l'espace public « au nom d'une cause » — en particulier la contestation des usages de la technologie jugés liberticides (Wray 1998 ; Jordan 2001 ; Jordan & Taylor 2004). Certaines initiatives qui en relèvent visent à divulguer des informations considérées comme étant d'intérêt public à travers le maniement de fuites d'informations, sur le modèle de WikiLeaks (Karatzogianni 2018). Mais ce type d'actions peut également être à l'initiative d'États visant à déstabiliser un pays tiers, comme l'ont montré les fuites de courriers électroniques d'équipes de campagnes lors des élections présidentielles américaines de 2016 (DNS email leak, Podesta email leak) et française de 2017 (MacronLeaks), attribuées à des hackers liés à l'État russe (Greenberg 2019). En effet, le *hacking* constitue aussi « *une ressource dans le déploiement du pouvoir étatique* » (Follis & Fish 2020, p. 9). Enfin, le politique vient également se loger dans des replis et interstices moins évidents ou moins ouvertement revendiqués.

3 En dépit de ces formes distinctes de rapport au politique, un trait partagé semble se dégager : le *hacking* — ainsi que la figure du hacker qui s'y rapporte — renvoie à la catégorie de ruse, au sens d'une intelligence pratique identifiée par Detienne et Vernant (1974). Cette piste prolonge une observation de Nicolas Auray, dans un travail pionnier (2000), pour qui la curiosité exploratoire et la virtuosité des hackers constituent à la fois un « *éveil critique* » et la manifestation d'une forme de pouvoir *sur* et *par* la technique. Différentes enquêtes sont mobilisées dans ce numéro, qui rendent compte des « *tactiques* » issues de la pratique quotidienne des acteurs (Certeau 1980) et qui soulignent la manière dont celles-ci visent à court-circuiter, à déjouer, à subvertir les forces en présence en recourant à l'ingéniosité voire à la manipulation plutôt qu'à l'accumulation de moyens matériels. Malgré la diversité de ses manifestations, nous faisons ainsi l'hypothèse que la ruse constitue une ressource commune ainsi qu'une disposition fondamentale des acteurs qui se réclament du *hacking*, et que cette catégorie peut éclairer la nature politique de leurs actions.

# De l'« éthique hacker » au pirate, une figure ambivalente

4 De même que l'être rusé se révèle à travers les ruses qu'il accomplit, le *hacking* comme pratique renvoie consubstantiellement au hacker, et aux qualités voire aux vertus que celui-ci manifesterait par ses actions. En effet, il est régulièrement fait référence à la figure « *du* » hacker, comme si un fil conducteur reliait ensemble les pratiques évoquées ci-dessus. Cette trame commune a initialement pris la forme d'une « éthique hacker », présentée dans le livre fondateur de Steven Levy (1984), qui affirme notamment l'ouverture à travers l'égalité d'accès aux ordinateurs, la liberté de circulation de l'information, le rejet de l'autorité et des bureaucraties, une méritocratie fondée sur les compétences pratiques, ainsi qu'une ambition esthétique et artistique et une capacité à « *changer sa vie pour le meilleur* ». L'histoire des *academic hackers,* retracée par Levy des années 1950 au début des années 1980 et du MIT à l'université de Stanford, est celle d'étudiants pour la plupart, qui se distinguent des autres ingénieurs et scientifiques par leur capacité à détourner les règles et à faire preuve de créativité.

5 Dans l'ouvrage de Levy, la transgression, le franchissement de certaines limites constituent déjà des éléments clés de la pratique hacker, qu'il s'agisse de crocheter les

serrures des salles où sont conservés les ordinateurs centraux de l'université, ou plus tard de s'opposer à l'application de la propriété intellectuelle au domaine du logiciel. Cependant une généalogie parallèle, plus éloignée des centres universitaires, met davantage l'accent sur des *illégalismes* hackers plus marqués tels que le *phreaking* (contraction de *phone* et *freak*) qui, dès les années 1970, consista à pénétrer les systèmes de communication téléphonique pour en connaître les secrets mais aussi profiter d'appels gratuits, et qui fut également l'une des matrices du *hacking* informatique (Coleman 2012 ; Lapsley 2013).

6 Le *hacking* est d'abord une catégorie émique définie par les acteurs eux-mêmes à travers des écrits ainsi que des modes d'interaction et de sociabilité très divers : des « manifestes » (*The Hacker Manifesto* par The Mentor, 1986 ) et des « glossaires » (*The Jargon File*, un fichier partagé entre différents auteurs à partir de 1975, puis publié sous le titre *The Hacker's Dictionary* en 1983) ; des magazines dédiés (*2600 : The Hacker Quarterly* fondé en 1984, *Phrak Magazine* lancé en 1985, et aujourd'hui de nombreuses publications en ligne) ; des clubs et des associations (comme le Homebrew Computer Club où bricolèrent les fondateurs de Apple Steve Jobs et Steve Wozniak au milieu des années 1970, ou encore le Chaos Computer Club lancé en Allemagne en 1981 et devenu une véritable institution) ; des centaines de conférences réunissant parfois des milliers de participants (Chaos Communication Congress, DEF CON etc.) ; des lieux de collaboration et de partage de ressources (les *hacklabs* et *hackerspaces* tels que les célèbres Metalab à Vienne et Noisebridge à San Francisco) ; des événements (les *hackathons* qui se présentent comme des compétitions de codage informatique, ou encore les *cryptoparties* pour former aux rudiments de la sécurité informatique) ; des listes de diffusion, des messageries IRC et des forums. Enfin le résultat de leurs actions est souvent directement observable : production de code et de protocoles (qui peuvent être partagés dans des *repositories*), de logiciels (qui deviennent parfois des projets collectifs d'ampleur, comme c'est le cas pour certains logiciels libres et *open source*), de licences alternatives, fuites d'informations etc.

7 Cependant, les premiers travaux sur les hackers sont en majorité des récits journalistiques et ils y sont présentés tour à tour comme des « héros » et des « sorciers » (Levy 1984 ; Hafner & Lyon 1996) capables d'affirmer leur autonomie face à la technique, ou comme des « hors-la-loi », des « clandestins » (*underground*) et des « pirates » résistant aux visées hégémoniques des grands opérateurs de télécommunications et des multinationales de l'informatique, à l'instrumentalisation du droit et à la répression policière (Hafner & Markoff 1991 ; Sterling 1992). Aux États-Unis, le Counterfeit Access Device and Computer Fraud and Abuse Act, adopté en 1984 et plusieurs fois amendé, est venu acter la notion de crime informatique, introduisant des sanctions sévères et souvent considérées comme disproportionnées eu égard aux torts commis ; initialement destiné à prévenir les intrusions dans les réseaux informatiques des institutions fédérales, il fut également instrumentalisé pour protéger les intérêts commerciaux privés, en ciblant non seulement l'accès non autorisé dans les systèmes mais également la modification et la copie de logiciels. L'image de « bandits populaires » fut renforcée par la publication de biographies et autobiographies à succès de certains hackers particulièrement doués qui furent traqués par les autorités, avant parfois de rejoindre l'industrie naissante de la sécurité informatique (Littman 1997a ; Littman 1997b ; Mitnick 2011).

8 Les représentations du *hacking* puisent également dans la fiction : l'un des romans fondateurs de la cyberculture qui a popularisé le terme de « cyberespace » a pour (anti-)héros un hacker mercenaire capable de quitter son enveloppe charnelle pour s'introduire dans les arcanes des grandes puissances monopolistiques en vue de « libérer » des intelligences artificielles (Gibson 1984). Dans les productions audiovisuelles qui le mettent en scène, depuis le célèbre *WarGames* (1983) jusqu'à la série *Mr. Robot* (2015-2019) louée pour son réalisme, on retrouve également cette image d'un individu talentueux mais moralement ambivalent, luttant contre un «

système » puissant mais faillible. La figure du hacker est donc souvent celle d'un David astucieux face aux Goliaths que sont les ordinateurs centraux, les logiciels et les réseaux de communication contrôlés par les puissances économiques ou militaires ; un acteur dominé à certains égards mais dont l'acuité et la connaissance intime des technologies est capable d'enrayer une technostructure centralisée et rationalisée à outrance. Dans ce rapport du faible au fort réside l'un des ressorts fondamentaux de la ruse : le faible est d'autant plus incité à user de ruse qu'il s'oppose à un « fort » et qu'il ne peut l'emporter par des moyens conventionnels. Il doit contourner l'obstacle, déjouer les pièges et surprendre l'adversaire s'il veut échapper à la domination (Holeindre, 2017).

9 Avec la généralisation de l'informatique personnelle et la montée en puissance du web dans les années 1990, chaque utilisateur a pu se représenter lui-même comme une cible potentielle des intrusions informatiques, des fuites d'information ou de la diffusion de virus. Les incitations économiques à commettre des larcins informatiques augmentèrent également avec la numérisation croissante des activités. L'image du hacker a ainsi connu des renversements successifs et oscillé à partir des années 1980 de celle d'« *ardents (bien qu'excentriques) programmeurs capables de brillantes et non-orthodoxes prouesses dans la manipulation des machines* » à celle de vandales, d'escrocs voire de terroristes encapuchonnés menaçant l'ordre établi depuis leur clavier (Nissenbaum 2004, p. 196). Ces représentations sont pour partie le fruit d'une criminalisation croissante des activités des hackers, participant à construire une forme de déviance (Jordan & Taylor 1998 ; Thomas 2002) mais qui a également contribué à en politiser les enjeux (Sterling 1992 ; Taylor 1999).

10 Le thème de la piraterie associé au *hacking* reflète cette ambiguïté, avec d'un côté la dimension romanesque de liberté, d'autonomie et d'exploration, affranchie des contraintes car hors d'atteinte de l'État ; et de l'autre le stigmate de « l'ennemi commun à tous », qui non seulement est en dehors des lois mais qui met celles-ci en danger. Il en va de même de la ruse, qui constitue à la fois une forme d'intelligence et de tromperie : d'une part, elle est valorisée car elle reflète les capacités cognitives et l'audace de celui qui l'emploie ; de l'autre, elle constitue une manœuvre déloyale, un contournement de la règle qui relève de la « tricherie » (Detienne & Vernant, 1974, p. 19-20). Mais ce stigmate peut être allègrement retourné : le hacker comme pirate rusé manifeste également avec force le « sens du juste » propre aux indigènes du numérique, qui les amène parfois à enfreindre une légalité perçue précisément comme injuste ou illégitime (Auray 2009). Le hacker adopte ainsi le visage du « justicier » qui contourne un système de droits de propriété intellectuelle qu'il juge inique, ou qui lance des actions directes (fuites de documents, dénonciations publiques, sabotages) contre les responsables de ce qu'il considère comme des abus de pouvoir, participant ainsi à (re-)politiser « *un monde qui, parce qu'il est technicisé, est menacé par la dépolitisation* » (*ibid.*, p. 173).

11 Le hacker-pirate transgresse en effet les règles (ou exploite les interstices entre les règles) en se revendiquant d'autres règles présentées comme plus légitimes, car tenant compte des spécificités de l'espace numérique : sa contestation des normes génère donc « *un processus conflictuel de construction des règles de l'espace numérique* » (Hayat et Paloque-Berges 2014). En outre, ce conflit est de haute intensité dans la mesure où les deux parties le situent hors du champ juridico-politique : le qualificatif de « pirate » vient justifier de la part des autorités un traitement d'exception, tandis qu'il manifeste pour ceux qui s'en revendiquent une rupture avec la société et parfois l'affirmation d'un modèle de société alternatif (*ibid.*). À l'issue de ce processus cependant et après avoir été les « *aiguillons* » et les « *renégats nécessaires* » du capitalisme qui le poussent à se renouveler et s'adapter, les anciens pirates peuvent aussi parfois rejoindre les rangs de sa « *machine souveraine* » (Durand & Vergne 2010).

12 Pour le dire dans les termes de Certeau (1980), le complexe État-entreprises développe une « *stratégie* » à travers le déploiement d'institutions, la planification

d'un système et la maîtrise d'un territoire. À l'inverse, le hacker, renvoyé aux marges, est par excellence celui qui parvient à tirer avantage de sa mobilité en exploitant les contingences et moments opportuns, s'opposant par nécessité de manière « *tactique* » — c'est-à-dire qui « *utilise, vigilante, les failles que les conjonctures particulières ouvrent dans la surveillance du pouvoir propriétaire* » (1980, p. 63). Pour y parvenir, il adopte ainsi des attitudes et fait appel à des compétences qu'il est possible de saisir à travers la notion de ruse.

## La subversion des normes ou le *hacking* comme intelligence rusée

13 Un volume croissant de recherches en *media studies*, en ethnologie, en sociologie, ou encore en histoire a permis d'affiner et d'approfondir la connaissance des mondes du *hacking*, soulignant la diversité des (contre-)cultures hackers. Par exemple, l'éclairage apporté sur les différentes « scènes » européennes du *hacking* dès l'apparition de l'ordinateur personnel (Alberts & Oldenziel 2014) vient nuancer une lecture excessivement centrée sur l'expérience des États-Unis. Les caractéristiques socio-démographiques des hackers — dispersés géographiquement, enclins à préserver leur anonymat, et évoluant souvent en dehors de toute organisation formelle — restent cependant difficiles à établir, d'autant qu'elles évoluent également au cours du temps. Beaucoup de travaux s'accordent à décrire un monde largement dominé par des hommes, généralement assez jeunes et issus des classes moyennes, qui se perçoivent comme *outsiders* et sont réunis autour d'une sous-culture commune avec ses rites de passage (Turkle 1984 ; Jordan & Taylor 1998 ; Steinmetz 2016). La juvénilité et l'entre-soi masculin expliquent en partie la construction d'une identité hacker fondée sur l'exploration, la compétition interne et la transgression (Ensmenger 2015). C'est le cas du moins dans la première partie de leur « carrière », lorsqu'ils sont le plus susceptibles de s'engager dans des activités illicites, avant de rallier le secteur de la sécurité informatique ou de poursuivre d'autres projets, parfois au prix d'une « identité dédoublée » (Auray & Kaminsky 2007).

14 La démonstration d'adresse technique constitue en effet un point central de l'appartenance hacker, qui explique également qu'elle soit structurée par une forme de méritocratie particulière : on est théoriquement jugé sur ce qu'on « fait » concrètement (« *code wins arguments* ») plutôt que sur des formes d'autorité institutionnelles (diplômes, statut social) — ce qui entraîne une hiérarchisation très forte des compétences. Un *hack* se distingue des autres actions liées à l'informatique et suscite l'admiration par sa virtuosité, sa créativité ou son habileté technique. Il s'agit donc de se démarquer du tout-venant et de gagner une forme de reconnaissance par les pairs, que ce soit par exemple sur les forums et listes de discussion ou au cours des conférences. À l'inverse, les *noobs* (néophytes) et les *script kiddies* qui glanent des solutions « clés en main » sur ces mêmes forums sont relégués tout au bas de l'échelle.

15 Ainsi, c'est avant tout par leurs pratiques que les hackers ont été approchés, et c'est également ce qui permet de dégager certains traits partagés. Comme nous l'avons dit le *hacking* a longtemps été associé à une forme d'autonomie individuelle, face à la technique d'abord, mais aussi par extension face aux systèmes sociaux et politiques (Jordan 2008). Cette idée fait écho aux enseignements de la sociologie des sciences et techniques, selon laquelle les scénarios qui guident l'interaction avec la technologie exercent certes une forme de pouvoir mais rarement une emprise complète, et se conçoivent toujours dans une relation dynamique avec les acteurs sociaux qui « bricolent » leur rapport aux objets (Akrich 1987 ; Oudshoorn & Pinch 2003), ce qui est particulièrement vrai de l'ordinateur personnel à ses débuts (Bardini & Horvath 1995). Cependant, au-delà d'un bidouillage ingénieux il s'agit également ici d'une

manière de remodeler les normes, et parfois de détourner des systèmes sociaux-techniques par des modifications matérielles, des innovations logicielles, l'exploitation de failles techniques, ou par des subterfuges qui ne relèvent pas du numérique *stricto sensu* (manipulation psychologique, dispositif juridique tel que le *copyleft*).

16 Comme l'a bien montré Nicolas Auray (2000), le *hacking* consiste non seulement à construire ou à co-construire l'objet technique, mais également à développer des stratagèmes pour conserver la maîtrise des interactions. Les hackers « *collectionnent* » des ruses — qui vont de quelques lignes de code aux techniques sophistiquées d'offuscation, réseaux de *botnets* (« machines zombies » contrôlées à distance), programmes de déverrouillage, *spoofing* (usurpation) d'adresses réseau, portes dérobées et autres chevaux de Troie — qui leur permettent d'anticiper des situations mais aussi de s'adapter aux contingences, en adaptant en permanence leurs boîtes à outils et leurs méthodes. Le *hacking* suppose de faire preuve à la fois de dextérité et d'opportunisme, en s'appuyant sur des connaissances éprouvées et une expérience concrète. Dans cette perspective, le *hacking* peut se comprendre comme une forme contemporaine d'« intelligence rusée », telle que Detienne et Vernant (1974) l'ont identifiée dans leur travail sur la *mètis* des Grecs. Selon eux, la ruse a pour caractéristique d'être « *engagée dans la pratique* » et n'est pas à proprement parler un concept, mais bien plutôt des « *comportements intellectuels qui combinent le flair, la sagacité, la prévision, la souplesse d'esprit, la feinte, la débrouillardise, l'attention vigilante, le sens de l'opportunité, des habiletés diverses, une expérience longuement acquise* » (*ibid.* p. 8 et 10).

17 Chez Lévi-Strauss déjà, le bricolage constitue un savoir d'expérience et une « *science du concret* » qui vient s'opposer au système conceptuel élaboré par l'ingénieur (Lévi-Strauss 1962, Ch. 1). Et pour Gabriella Coleman, qui s'est intéressée en anthropologue à une diversité de cultures hacker allant des logiciels libres (2013) au mouvement des Anonymous (2014), le *hacking* se situe au point de convergence de l'artisanat (*craft*) et de l'artifice / l'astuce / la ruse (*craftiness*), jouant sur la proximité de ces termes en anglais (2013 ; 2016 ; 2017). Selon elle, cet alignement « *est peut-être le meilleur endroit pour trouver un fil unificateur courant à travers la diversité des mondes techniques et éthiques du hacking* » (2017, p. 162) voire un « *universel du hacking* » (*ibid.,* p. 164).

18 La notion d'artisanat (*craft*), par opposition au monde industriel, implique un savoir-faire qui appartient en propre à l'individu ainsi qu'une production matérielle dont il reste maître. Elle renvoie également au partage d'outils, de ressources et de techniques, à la transmission de règles empiriques et de normes d'usage, et aux gestes affutés par la pratique. Elle est associée enfin à une forme d'exigence à l'égard du travail réalisé, qui constitue sa propre finalité et sa valeur et qui prime sur le profit qu'il est possible d'en tirer. L'astuce ou l'artifice (*craftiness*) se présente davantage comme une « *disposition esthétique* » (*ibid.*, p. 163) pour la créativité, l'originalité mais aussi le jeu et parfois la duperie, qui s'exprime par exemple à travers des formes d'humour, de farces et de canulars (parfois inscrits dans le code informatique lui-même). Dans son ouvrage sur les Anonymous (2014), Coleman fait même du hacker une déclinaison contemporaine de l'archétype mythologique du *trickster* (le fripon ou « joueur de tours ») qui, du dieu grec Dionysos à la fée facétieuse du folklore celte, peut aussi bien divulguer des connaissances que semer le doute et la confusion, bousculant l'ordre des choses par son imprévisibilité. Le *trickster* est à la culture mythologique ce que le hacker est à la culture numérique : une figure de la transgression, du trouble, de l'ingéniosité, de la remise en cause des hiérarchies établies et du pouvoir en place.

## Les ruses politiques du *hacking*

19 Coleman souligne cependant que ce dénominateur commun ne permet pas à lui seul de qualifier le sens et les finalités politiques du *hacking*. L'orientation idéologique des hackers est souvent réduite à une adhésion simpliste au libertarianisme. Mais si celle-ci renvoie à la sensibilité aiguë que les hackers peuvent manifester s'agissant des enjeux liés à la vie privée, à l'autonomie individuelle ou à la liberté d'expression, elle n'est pas suffisante pour caractériser l'ensemble des pratiques individuelles, des sous-genres et des déclinaisons régionales du *hacking* (Coleman 2016). Certains hackers revendiquent ainsi une position autonomiste, d'autres une vision anarcho-capitaliste, tandis que d'autres encore s'accordent parfaitement avec un libéralisme marchand classique — ou bien privilégient tout simplement leur intérêt individuel. S'ils partagent généralement une sensibilité commune de nature « libérale », celle-ci trouve différentes « expressions morales » et leurs valeurs et leurs engagements peuvent être radicalement opposés (Coleman & Golub 2008).

20 Toutefois, une attention plus précise aux types de ruses choisies, aux interactions avec d'autres institutions productrices de normes (au premier rang desquelles l'État et le marché) et aux controverses qu'elles suscitent, peut permettre de s'affranchir d'une lecture avant tout morale des actions menées par les hackers, et de mieux éclairer leur nature politique. À ce titre, le bouleversement de la propriété intellectuelle par l'informatisation constitue une épreuve fondatrice pour les hackers. Il les a contraints soit à se ranger au nouveau cadre juridique mis en place au cours des années 1980, soit à le « renverser » de l'intérieur (notamment par les logiciels et licences libres), soit à se soustraire complètement au droit (par exemple en déverrouillant l'accès aux contenus protégés, et en ayant recours à des technologies de partage décentralisé de fichiers et de biens culturels tels que le *peer-to-peer*). Il constitue ainsi l'un des moments charnières où se dessinent les différentes interprétations de la « liberté » propre au « *libéralisme informationnel* » qui caractérise l'avènement du numérique (Loveluck 2015, Ch. 6).

21 Pour certains auteurs, les hackers constituent même une forme d'avant-garde ou d'élite voire une « classe révolutionnaire » défiant le capitalisme informationnel (Wark 2004 ; Söderberg 2008) — bien que les innovations des hackers et leur expertise soient parfaitement susceptibles d'être « récupérées » par des entreprises commerciales ou des entités politiques (Delfanti & Söderberg 2018). Pour d'autres au contraire, « l'éthique hacker » constitue un nouvel « esprit du capitalisme » à l'ère informationnelle, fondé notamment sur des relations de travail autonomes, coopératives et motivées par le plaisir (Himanen 2001). Il s'agit dans les deux cas de lectures « idéalistes » du *hacking* (Jordan 2008), très sélectives et qui, prises ensemble, apparaissent contradictoires. Mais elles illustrent la manière dont le refus de se plier aux contraintes édictées et le recours à l'ingéniosité pour s'en extraire politisent d'un même mouvement les enjeux de la technique, non seulement en posant très ouvertement la question » qui contrôle le code ? » mais en produisant des alternatives concrètes.

22 Par ailleurs, les ruses du *hacking* revêtent également une dimension politique par les formes organisationnelles et les modes de gouvernance inédits qui se mettent parfois en place à travers ces alternatives, comme c'est notamment le cas dans certains projets de logiciels libres tels que Debian dont les innovations institutionnelles ont été bien étudiées (Weber 2004 ; Auray 2007 ; Demazière, Horn et Zune 2007 ; Lazaro 2008 ; Broca 2013 ; Coleman 2013) ou dans les *hackerspaces* qui privilégient des formes horizontales de gouvernance (Maxigas 2012 ; Lallement 2015).

23 Mais c'est la notion de *hacktivisme* évoquée plus haut qui constitue l'une des formes paradigmatiques du « *hacking* politique », malgré ses ambivalences. Elle recouvre notamment des actions de sabotage, de blocage, ou de fuite d'informations (*leaks*) visant à attirer l'attention sur un enjeu politique ou social, que leurs auteurs présentent comme une forme de désobéissance civile. Selon le contexte politique et

les objectifs visés, un large « répertoire d'actions numériques » (Van Laer & Van Aelst 2010) peut être mobilisé : intrusions, attaques dites « par déni de service » (DDoS), tactiques d'anonymisation et d'offuscation (utilisation de messageries chiffrées, réseaux décentralisés), stratégies de délocalisation des infrastructures matérielles etc. Dans certains cas la démonstration d'une faille de sécurité est une manière d'exposer les vulnérabilités d'une institution — y compris par exemple en « cambriolant » publiquement une banque (avant de restituer aussitôt les fonds déplacés) pour démontrer les lacunes du système de communications électroniques mis en place par le service national des postes allemand, comme le fit le Chaos Computer Club en 1984. Le *hacking* peut ainsi se présenter comme vigie démocratique et conscience collective des conséquences sociales des technologies, voire comme une alerte face à des dérives autoritaires (Webb 2020).

24 Comme le formule également Nicolas Auray, le questionnement des institutions est central chez les hackers : « *Ils cherchent à "percer", à casser une réalité qu'ils considèrent comme dissimulatrice, et donc à faire émerger une discontinuité entre deux manières de décrire la même réalité. Ils tentent aussi d'échafauder des institutions alternatives* » (2013, p. 12). En effet, le *hacking* peut également constituer une rupture plus radicale avec les institutions existantes. Au cours des années 1990, une association nouvellement créée de défense des libertés numériques (l'Electronic Frontier Foundation) ainsi qu'un groupe de hackers appelés *cypherpunks*1 ont ouvertement défié l'État au cours de ce qu'on a appelé les *crypto wars* (Levy 2001). Il s'agissait de lutter contre l'affaiblissement délibéré des technologies de chiffrement, et de promouvoir la cryptographie et les réseaux anonymisés permettant d'assurer la confidentialité des échanges privés. Pour les *cypherpunks*[1] — qui furent par exemple rejoints par le fondateur de WikiLeaks Julian Assange — l'enjeu consistait même à poser les bases technologiques d'une sécession des structures régaliennes voire d'une « crypto anarchie » (Greenberg 2012). Les techniques de chiffrement à clé publique tels que PGP (*Pretty Good Privacy*) furent présentés comme un savoir/pouvoir dont chacun devrait pouvoir disposer, des formules mathématiques ou des « lois physiques » que l'État malgré ses ressources colossales serait incapable de « casser » : une « arme du faible » qui permettrait à l'individu de garantir sa propre « protection » et son autonomie (Assange et al. 2012). Plus récemment, cette ambition s'est traduite sur le plan bancaire et financier par le développement de cryptomonnaies telles que Bitcoin, qui ne seraient plus adossées à des institutions étatiques (De Filippi & Loveluck 2016).

25 Enfin à l'inverse, le *hacking* peut être consacré à la défense des intérêts régaliens, y compris militaires, lorsque des hackers mettent leurs compétences au service de l'État à des fins de renseignement, de dissuasion, de déstabilisation voire pour mener des actions offensives (Buchanan 2020). Cette dernière manifestation du *hacking* a pour l'instant été relativement peu prise en compte par la littérature existante, dans la mesure où elle contrevient à la représentation libertaire du hacker. Certains auteurs ont cependant bien mis en évidence le « travail des frontières » entrepris par les États qui cherchent à réaligner le *hacking* avec leurs objectifs propres — d'un côté en stigmatisant et en criminalisant certaines formes d'activisme hacker qui contestent l'État, et de l'autre en co-optant les hackers et en construisant une forme légitime de « *hacking* éthique » dirigé vers la « cybersécurité » et largement investi par le secteur privé (Follis & Fish 2020 ; voir également Jordan & Taylor 2004). Les modalités d'implication des autorités avec les hackers peuvent être plus ou moins officielles (Maurer 2018), et si certains sont directement employés par des agences gouvernementales, d'autres peuvent être simplement mandatés, ou bien même opérer avec leur accord tacite : lorsque des hackers, par le degré de sophistication de leurs actions, entrent dans les radars des autorités, il devient possible soit d'essayer de les arrêter, soit de les recruter lorsque c'est possible, soit de les laisser poursuivre leurs activités mais en ayant recours à leurs services dans certaines situations. Les pirates se font ici corsaires ou flibustiers, cette dernière situation étant avantageuse

— et pouvant même être considérée comme une ruse en soi — car autorisant une grande souplesse et une capacité de « déni plausible » lors d'opérations de renseignement ou d'actions offensives.

26 La gamme des techniques mises en œuvre est très large, toute la palette tactique et stratégique étant mobilisée. Elle recouvre par exemple des cyberattaques sophistiquées, telles que le ver Stuxnet lancé en 2010 pour neutraliser les centrifugeuses d'enrichissement d'uranium en Iran, ou encore NotPetya qui a paralysé de nombreux systèmes informatiques en Ukraine en 2017 avant de se diffuser partout dans le monde, et qui combinait de nombreuses ruses : ce « crypto-ver » ou « crypto-virus » (logiciel de chiffrement de données capable de se diffuser de manière autonome sur les réseaux informatiques) s'est fait passer pour un « rançongiciel » (qui implique l'extorsion d'une somme en Bitcoins en échange du déchiffrement des données), mobilisait plusieurs failles critiques inconnues (également appelées *zero-days*) de Windows précédemment « volées » aux hackers de la NSA, et s'est initialement diffusé suite à l'infection de la mise à jour d'un logiciel de comptabilité équipant la majorité des entreprises ukrainiennes ainsi que des banques et des ministères (Greenberg 2019).

27 Au-delà de ces cas exceptionnels, le recours aux hackers prend également d'autres formes, plus banalisées et où les ruses employées peuvent être plus rudimentaires mais bien rodées. Le Citizen Lab (Université de Toronto) qui étudie et dénonce la surveillance ainsi que la censure d'internet, vise également à rendre compte des attaques informatiques ciblant des membres de la société civile (journalistes, militants, opposants politiques) et qui sont donc généralement motivées politiquement. Le centre publie de nombreux rapports[2] permettant de recenser les attaques connues et détaillant les techniques employées, les acteurs impliqués et les cibles visées — journalistes mexicains, diaspora tibétaine, ONG en Égypte etc. Citizen Lab a par exemple montré l'existence de ce qui peut être qualifié de *hack-for-hire* ou *hacking as a service* : des entreprises qui prospectent auprès de tous types de clients — publics ou privés — et qui ne travaillent pas nécessairement avec un haut degré de sophistication mais se déploient à grande échelle. Elles ont le plus souvent recours au *spear-phishing* : un hameçonnage ciblé à partir de messages contenant des liens piégés, permettant soit d'installer des logiciels espions soit tout simplement de récupérer des identifiants. Une enquête a montré que des milliers d'individus dans de nombreux pays — journalistes, responsables politiques, syndicalistes et militants d'ONG, juges et avocats, industriels, investisseurs financiers — ont été pris pour cible pendant des années, vraisemblablement par l'entreprise indienne BellTroX Infotech pour le compte de ses clients (Scott-Railton et al. 2020). L'entreprise faisait tout à fait ouvertement la promotion de ses services, qui pouvaient être déployés aussi bien dans le cadre d'affaires judiciaires, de campagnes politiques, d'opérations financières ou encore de relations publiques. Des personnes impliquées dans la campagne #ExxonKnew, dénonçant l'attitude du groupe pétrolier ExxonMobil qui aurait caché des informations sur le changement climatique depuis des dizaines d'années, ont par exemple été visées.

## Pragmatique du *hacking*

28 À travers les contributions réunies pour ce dossier thématique, il s'agit donc d'interroger les pratiques du *hacking* sous l'angle de l'intelligence rusée des acteurs, tout en évaluant la portée politique de leurs actions. Peut-on parler de « politiques du *hacking* » au sens où le champ numérique se prêterait particulièrement à ce type d'intelligence rusée faite de bidouillages et de contournements ingénieux ? Quelle grammaire du *hacking* la ruse dessine-t-elle et dans quelle mesure se présente-t-elle comme une ressource pour les acteurs, une compétence acquise en réponse aux

épreuves auxquelles ils sont confrontés, ou encore comme un instrument de lutte dans un contexte d'asymétries d'informations ou de capacités ? Quelles sont les controverses soulevées par le recours à telle ou telle ruse ? Les contributions au dossier visent ainsi à questionner le sens de ces pratiques en tant que manifestation de pouvoirs individuels ou collectifs. Il s'agit de montrer que les ruses et leur contexte historique et social de déploiement (ou d'empêchement) constituent une entrée privilégiée pour engager une *pragmatique du hacking* qui en révèle les enjeux politiques.

29 L'article de Félix Tréguer rappelle ainsi qu'une veine anti-technocratique du hacktivisme puise ses racines dans le mouvement de la Nouvelle Gauche des années 60, et souligne la portée « anti-hégémonique » de différentes formes d'action directe allant de la fuite d'informations au sabotage. Il montre également que la vague répressive contre les hackers de la fin des années 1980 visait non seulement à criminaliser les intrusions informatiques, mais plus largement à discipliner des pratiques pouvant remettre en cause le déploiement de « sociétés de contrôle », et ce au prix d'un « traitement d'exception » réservé à l'action politique sur Internet qui a durablement affaibli cette frange militante du hacktivisme.

30 Symétriquement, Olivier Alexandre montre qu'en dépit de la sensibilité « anti-système » des hackers, leur sens tactique constitue une source centrale d'innovation pour la Silicon Valley. Il détaille les stratégies déployées par les entreprises de la *big tech* pour capter ces pourvoyeurs de « disruption ». En s'alignant sur leurs valeurs, en éludant la dimension commerciale à travers des stratégies de « postvaluation », ou encore en s'appuyant sur leurs infrastructures et environnement techniques — en particulier les logiciels libres — le capitalisme numérique est ainsi parvenu à instaurer « *une relation d'interaction et de co-dépendance* » avec les hackers.

31 Dans un autre contexte politique, en s'intéressant aux intermédiaires techniques de l'internet Russe, Ksenia Ermoshina et Francesca Musiani présentent les ruses auxquelles ils ont recours afin d'éluder les dispositifs juridico-techniques que l'État russe voudrait imposer à des fins de surveillance et de censure, mais qui introduisent des contraintes techniques fortes (et parfois aberrantes) ainsi qu'une charge financière conséquente. Ermoshina et Musiani montrent aussi comment ces ruses témoignent d'une attention (*care*) des acteurs pour le milieu dont ils ont une connaissance intime et dont ils tirent également leurs moyens de subsistance, cherchant ainsi à le préserver tout en évitant une opposition frontale au gouvernement et à la régulation. Elles soulignent enfin que c'est la nécessité même de devoir recourir à des ruses et mettre en œuvre des stratagèmes de contournement, de résistance ou de contestation, qui politise ces acteurs techniques et économiques.

32 Benjamin Loveluck revient pour sa part sur le mouvement Anonymous, dont l'ambivalence incarne de manière exemplaire la dualité de la ruse, conçue à la fois comme intelligence créatrice et comme tromperie délétère. Il montre que la diversité des actions entreprises, si elles peuvent parfois se comprendre comme la défense d'une cause publique, relèvent également du vigilantisme et de l'auto-justice. En conséquence, le mouvement demeure cantonné aux frontières de l'engagement politique dans la mesure où la portée de ses actions, évaluées avant tout selon leurs finalités, demeure tributaire de catégorisations morales.

33 Estéban Georgelin et Jean-Vincent Holeindre montrent enfin comment les compétences du *hacking* sont intégrées par les États eux-mêmes, qui recrutent des hackers pour s'approprier leur savoir-faire « technico-tactique » et les mobiliser dans le cadre d'une stratégie à plus grande échelle. Le rôle de ces hackers intégrés au système de défense des États (ou travaillant pour eux) est particulièrement fort compte tenu de la montée en puissance des formes non cinétiques de la guerre. Il existe une convergence entre le savoir-faire « rusé » des hackers, combinant transgression et ingéniosité, et la stratégie des États, qui repose de plus en plus sur la « gestion des perceptions » et des formes indirectes (et discrètes) d'affrontement. Dans le contexte stratégique actuel, la ruse est d'autant plus employée que l'usage de

la force est contraint politiquement, juridiquement voire économiquement ; ces « ruses de guerre numériques » permettent aux États à la fois de se protéger des attaques (action défensive) et de déstabiliser les autres États en usant dans certains cas de l'intoxication (action offensive).

---

## *Bibliographie*


M. Akrich, « Comment décrire les objets techniques ? », *Techniques & culture* n°9, 1987, p. 49-64.
DOI : 10.4000/tc.4999

G. Alberts et R. Oldenziel (dir.), *Hacking Europe. From Computer Cultures to Demoscenes,* London, Springer, 2014.

J. Assange, J. Appelbaum, A. Müller-Maguhn, et J. Zimmermann, *Cypherpunks. Freedom and the Future of the Internet*, New York, OR Books, 2012.

N. Auray, *Politique de l'informatique et de l'information. Les pionniers de la nouvelle frontière électronique,* thèse de doctorat de sociologie, EHESS, Paris, 2000.

N. Auray, « Le modèle souverainiste des communautés en ligne. Impératif participatif et désacralisation du vote », *Hermès* n° 47, 2007, p. 137-144.

N. Auray, « Pirates en réseau : détournement, prédation et exigence de justice », *Esprit* n 356, 2009, p. 168-179.

N. Auray, *Une enquête sur les institutions. Le hacker, l'État et la politique,* mémoire d'habilitation à diriger des recherches, université Nice Sophia-Antipolis, décembre 2013.

N. Auray et D. Kaminsky, « The professionalisation paths of hackers in IT security : the sociology of a divided identity », *Annales des télécommunications* vol. 62, n°11-12, 2007, p. 1312-1326.

T. Bardini et A. T. Horvath, « The social construction of the personal computer user : the rise and fall of the reflexive user », *Journal of Communication* vol. 45, n° 3, 1995-9, p. 40-66.

S. Broca, *Utopie du logiciel libre. Du bricolage informatique à la réinvention sociale,* Neuvy-en-Champagne, Le Passager clandestin, 2013.

B. Buchanan, *The Hacker and the State. Cyber Attacks and the New Normal of Geopolitics,* Cambridge, MA and London, Harvard University Press, 2020.

M. de Certeau, *Arts de faire : l'invention du quotidien,* Paris, Gallimard, 1980.

G. Coleman, « Phreaks, hackers, and trolls. The politics of transgression and spectacle », in M. Mandiberg (dir.), *The Social Media Reader,* New York and London, New York University Press, 2012, p. 99-119.

G. Coleman, *Coding Freedom. The Ethics and Aesthetics of Hacking,* Princeton, NJ, Princeton University Press, 2013.

G. Coleman, *Hacker, Hoaxer, Whistleblower, Spy. The Story of Anonymous,* London and New York, Verso, 2014.

G. Coleman, « Hacker », in B. Peters (dir.), *Digital Keywords. A Vocabulary of Information Society and Culture,* Princeton, NJ and Oxford, Princeton University Press, 2016, p. 158-172.

G. Coleman, « From Internet farming to weapons of the geek », *Current Anthropology* vol. 58, n°supplement 15, 2017, p. 91-102.
DOI : 10.1086/688697

G. Coleman et A. Golub, « Hacker practice. Moral genres and the cultural articulation of liberalism », *Anthropological Theory* vol. 8, n° 3, 2008, p. 255-277.

J. Crabtree, « Civic hacking : a new agenda for e-democracy », *openDemocracy*, 12 juin 2007 (https://www.opendemocracy.net/en/civic_hacking_a_new_agenda_for_e_democracy/, consulté le 2 mars 2021).

P. De Filippi et B. Loveluck, « The invisible politics of Bitcoin : governance crisis of a decentralised infrastructure », *Internet Policy Review vol.* 5, n° 3, 2016.

A. Delfanti et J. Söderberg, « Repurposing the hacker : three cycles of recuperation in the evolution of hacking and capitalism », *Ephemera vol.* 18, n°3, 2018, p. 457-476.

D. Demazière, F. Horn, et M. Zune, « Des relations de travail sans règles ? L'énigme de la production de logiciels libres », *Sociétés contemporaines* n 2, 2007, p. 101-125.

M. Detienne et J.-P. Vernant, *Les Ruses de l'intelligence. La mètis des Grecs,* Paris, Flammarion, 1974.

R. Durand et J.-P. Vergne, *L'Organisation pirate. Essai sur l'évolution du capitalisme,* Lormont, Le Bord de l'eau, 2010.

N. Ensmenger, « "Beards, sandals, and other signs of rugged individualism" : masculine culture within the computing professions », *Osiris* vol. 30, n 1, 2015, p. 38-65.

K. Ermoshina, « Civic hacking. Redefining hackers and civic participation », *Tecnoscienza* vol. 9, n 1, 2018, p. 79-101.

L. Follis et A. Fish, *Hacker States,* Cambridge, MA, MIT Press, 2020.
DOI : 10.7551/mitpress/11844.001.0001

W. Gibson, *Neuromancer,* New York, Ace Books, 1984.

A. Greenberg, *This Machine Kills Secrets. How WikiLeakers, Cypherpunks, and Hacktivists Aim to Free the World's Information,* New York, Dutton, 2012.

A. Greenberg, *Sandworm. A New Era of Cyberwar and the Hunt for the Kremlin's Most Dangerous Hackers,* New York, Doubleday, 2019.

K. Hafner et J. Markoff, *Cyberpunk. Outlaws and Hackers on the Computer Frontier,* London, Fourth Estate, 1991.

K. Hafner et M. Lyon, *Where Wizards Stay Up Late. The Origins of the Internet,* New York, Simon & Schuster, 1996.

S. Hayat et C. Paloque-Berges, « Transgressions pirates », *Tracés* n 26, 2014, p. 7-19.

P. Himanen, T*he Hacker Ethic and the Spirit of the Information Age*, New York, Random House, 2001.

J.-V. Holeindre, *La ruse et la force. Une autre histoire de la stratégie,* Paris, Perrin, 2017.

T. Jordan, *Activism ! Direct Action, Hacktivism and the Future of Society,* London, Reaktion Books, 2001.

T. Jordan, *Hacking. Digital Media and Technological Determinism,* Cambridge and Malden, MA, Polity Press, 2008.

T. Jordan et P.A. Taylor, « A sociology of hackers », *The Sociological Review vol.* 46, n 4, 1998, p. 757-780.
DOI : 10.1111/1467-954X.00139

T. Jordan et P.A. Taylor, *Hacktivism and Cyberwars. Rebels With A Cause ?*, London and New York, Routledge, 2004.

A. Karatzogianni, « Leaktivism and its discontents », in G. Meikle (dir.), *The Routledge Companion to Media and Activism,* London and New York, Routledge, 2018, p. 250-258.

P. Lapsley, *Exploding the Phone. The Untold Story of the Teenagers and Outlaws who Hacked Ma Bell*, New York, Grove Press, 2013.

C. Lazaro, *La Liberté logicielle. Une ethnographie des pratiques d'échange et de coopération au sein de la communauté Debian,* Louvain-la-Neuve, Bruylant-Academia, 2008.

C. Lévi-Stauss, *La Pensée sauvage,* Paris, Plon, 1962.

S. Levy, *Hackers. Heroes of the Computer Revolution,* Sebastopol, CA, O'Reilly Media, [1984] 2010.

S. Levy, Crypto. *How the Code Rebels Beat the Government—Saving Privacy in the Digital Age,* New York, Viking, 2001.

J. Littman, *The Watchman. The Twisted Life and Crimes of Serial Hacker Kevin Poulsen,* New York, Little Brown, 1997a.

J. Littman, *The Fugitive Game. Online With Kevin Mitnick,* New York, Little, Brown & Co., 1997b.

B. Loveluck, *Réseaux, libertés et contrôle. Une généalogie politique d'internet,* Paris, Armand Colin, 2015.

T. Maurer, *Cyber Mercenaries. The State, Hackers, and Power,* Cambridge and New York, Cambridge University Press, 2018.

P. Maxigas, « Hacklabs and hackerspaces : Tracing two genealogies », *Journal of Peer Production* n°2, 2012.

K. Mitnick, *Ghost in the Wires. My Adventures as the World's Most Wanted Hacker,* New York, Little, Brown & Co., 2011.

H. Nissenbaum, « Hackers and the contested ontology of cyberspace », *New Media & Society* vol. 6, n° 2, 2004, p. 195-217.
DOI : 10.1177/1461444804041445

N. Oudshoorn et T. J. Pinch (dir.), *How Users Matter. The Co-Construction of Users and*

*Technology,* Cambridge, MA and London, MIT Press, 2003.

A. Powell, « Hacking in the public interest : authority, legitimacy, means, and ends », *New Media & Society* vol. 18, n° 4, 2016, p. 600-616.
DOI : 10.1177/1461444816629470

A. R. Schrock, « Civic hacking as data activism and advocacy : a history from publicity to open government data », *New Media & Society* vol. 18, n 4, 2016, p. 581-599.

J. Scott-Railton, A. Hulcoop, B. A. Razzak, B. Marczack, S. Anstis, et R. J. Deibert, « Dark Basin. Uncovering a massive hack-for-hire operation », *Citizen Lab report,* 9 juin 2020 (https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/, consulté le 9 mars 2021).

J. Söderberg, *Hacking Capitalism. The Free and Open Source Software Movement,* London, Routledge, 2008.

K. F. Steinmetz, *Hacked. A Radical Approach to Hacker Culture and Crime,* New York, New York University Press, 2016.

B. Sterling, *The Hacker Crackdown. Law and Disorder on the Electronic Frontier,* London, Viking, 1992.

P. A. Taylor, *Hackers. Crime in the Digital Sublime,* London and New York, Routledge, 1999.

D. Thomas, *Hacker Culture,* Minneapolis, MN, University of Minnesota Press, 2002.

S. Turkle, *The Second Self. Computers and the Human Spirit,* New York, Simon & Schuster, 1984.

J. Van Laer et P. Van Aelst, « Internet and social movement action repertoires. Opportunities and limitations », *Information, Communication & Society* vol. 13, n°8, 2010, p. 1146-1171.

M. Wark, *A Hacker Manifesto,* Cambridge, MA, Harvard University Press, 2004.

S. Weber, *The Success of Open Source,* Cambridge, MA, Harvard University Press, 2004.

S. Wray, « Electronic civil disobedience and the World Wide Web of hacktivism », *Switch* vol. 4, n 2, 1998 (http://switch.sjsu.edu/web/v4n2/stefan/wp/v28.1.html).

## *Notes*

1 Contraction de cyber, *cipher* (chiffrement) et *punk* (voyou) — qui renvoie également à un genre de la science-fiction, le cyberpunk, qui combine le roman noir, la dystopie et les technologies informatiques, et dont William Gibson et Bruce Sterling mentionnés ici sont des auteurs phares.

2 https://citizenlab.ca/category/research/targeted-threats/

## *Pour citer cet article*

*Référence papier*
Benjamin Loveluck et Jean-Vincent Holeindre, « Politiques du *hacking* : enquête sur les ruses numériques », *Quaderni*, 103 | 2021, 9-24.

*Référence électronique*
Benjamin Loveluck et Jean-Vincent Holeindre, « Politiques du *hacking* : enquête sur les ruses numériques », *Quaderni* [En ligne], 103 | Printemps 2021, mis en ligne le 15 juin 2021, consulté le 10 septembre 2021. URL : http://journals.openedition.org/quaderni/1970 ; DOI : https://doi.org/10.4000/quaderni.1970

## *Auteurs*

**Benjamin Loveluck**
i3-SES/Télécom Paris

*Articles du même auteur*

**Les ruses du hacktivisme, aux frontières de l'engagement politique : retour sur Anonymous** [Accès restreint]
Paru dans *Quaderni*, 103 | Printemps 2021

**Jean-Vincent Holeindre**
Université Paris 2/Centre Thucydide et IRSEM

*Articles du même auteur*

**Des ruses de guerre numériques ? Le *hacking* comme ressource stratégique dans les conflits contemporains** [Accès restreint]
Paru dans *Quaderni*, 103 | Printemps 2021

## *Droits d'auteur*