

# TERMES

VOLET 2

HIVER 2021

# Vulnérabilité

Yuan Stevens  
*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

Elizabeth Vander Zaag  
*Digit Reproduces  
Digit and Man  
Through the Holes*

Anne-Marie Trépanier  
*«An infinity of solutions». Tactiques  
de résilience technologique dans  
les vidéos d'Elizabeth Vander Zaag*

# Yuan Stevens

*Résilience et capacité  
de survie:  
un regard sur les  
fenêtres de  
vulnérabilité*

## TERMES

1. Sharla P. Boehm et Paul Baran, *On Distributed Communications: II. Digital Simulation of Hot-Potato Routing in a Broadband Distributed Communications Network*, Santa Monica, CA, RAND Corporation, 1964, [https://www.rand.org/pubs/research\\_memoranda/RM3103.html](https://www.rand.org/pubs/research_memoranda/RM3103.html).

Yuan Stevens  
*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

Derrière le terme informatique de « vulnérabilité » se cache la présomption tacite que ce sont les systèmes informatiques et les données qu'ils renferment qui doivent être protégés d'intrusions potentielles. Pourtant, en examinant de près le terme et son évolution au fil du temps, on entrevoit un passé et un avenir riches en rebondissements comportant des conséquences de taille pour les populations dites vulnérables.

### CONFIGURER LA VULNÉRABILITÉ

La première occurrence présumée du terme de vulnérabilité dans le secteur de l'informatique moderne remonte aux années 1960. Dans un texte rédigé à l'intention de RAND, un *think tank* militaire américain, Sharla Boehm et Paul Baran avançaient des solutions pour assurer la survie et la résilience des systèmes de communication des forces aériennes à l'apogée de la guerre froide. Dans cet article fondateur paru en 1964, les deux informaticiens proposaient une nouvelle approche radicale : la mise sur pied d'un modèle décentralisé pour partager les données communiquées<sup>1</sup>.

## TERMES

2. Stewart Brand, « Founding Father », *Wired*, 1 mars 2001, <https://www.wired.com/2001/03/baran/>.
3. Paul Baran, *Reliable Digital Communications Systems Using Unreliable Network Repeater Nodes*, Santa Monica, CA, RAND Corporation, 1960, <https://www.rand.org/pubs/papers/P1995.html>.

Yuan Stevens  
*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

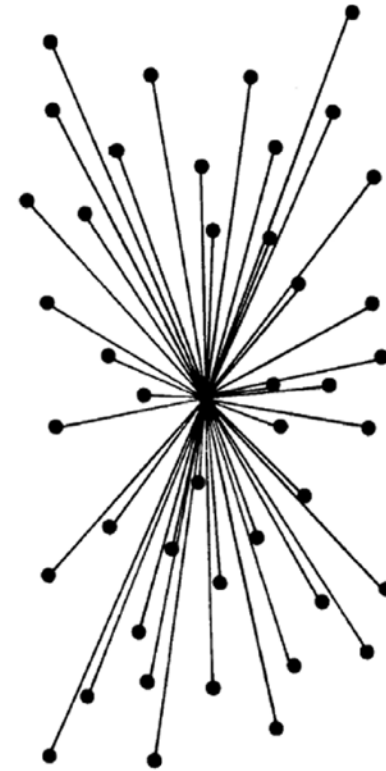


Figure 1: Réseau de communications analogique centralisé de Boehm et Baran (Source : RAND Corporation Memorandum RM-3420-PR, août 1964, 2.)

À l'époque, les systèmes de communication transféraient les données des messages dépêchés d'un lieu à un autre en employant des technologies analogiques permettant un transfert complet et immédiat<sup>2</sup>. Or dans un précédent rapport, Baran (en se basant sur le travail de Boehm, née Perrine) affirmait qu'un attentat nucléaire menaçait de détruire le système analogique alors en circulation partout sur la planète, et d'effacer ainsi des messages en route vers leur destination<sup>3</sup>.

4. *Ibid.*, p. 7.
5. *Ibid.*
6. Boehm et Baran, *On Distributed Communications*; Roy Rosenzweig, « Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet », *The American Historical Review*, vol. 103, n° 5, 1998, p. 1530-1552, doi:10.2307/2649970.

Yuan Stevens  
*Résilience et capacité de survie :  
 un regard sur les fenêtres de  
 vulnérabilité*

Selon Baran, l'infrastructure gouvernementale avait un criant besoin de protection. « Un système [distribué] », écrivait-il, « serait très utile pour préserver nos institutions démocratiques à la suite d'une possible attaque nucléaire<sup>4</sup> ». La proposition de Boehm et de Baran visait à « minimiser la vulnérabilité<sup>5</sup> » dans le contexte de la guerre froide, où il était crucial de protéger l'infrastructure du gouvernement américain.

La solution de Boehm et de Baran a eu pour effet de cerner les avantages de ce qu'on appelle aujourd'hui la « commutation de paquets<sup>6</sup> ». Pour le dire simplement, le système analogique centralisé partage un livre complet à la fois, tandis que le modèle numérique distribué envoie des pages (c.-à-d. des paquets de données) au fil du temps, qui sont par la suite assemblées à leur arrivée à destination. La commutation de paquets protège donc contre la destruction totale de l'information au moment de son transfert.

À la fin des années 1960, l'armée américaine a finalement mis en pratique le travail de Boehm et de Baran. Le département de la Défense s'est lancé dans l'élaboration de son propre réseau de communications et a financé l'Advanced Research Projects Agency (ARPA) en

7. *Ibid.*
8. *Ibid.*
9. *Ibid.*
10. Rosenzweig, « Wizards, Bureaucrats, Warriors, and Hackers », p. 1530-1552 ; Claire L. Evans, *Broad Band: The Untold Story of the Women Who Made the Internet*, New York, Portfolio/Penguin, 2018, p. 179.

Yuan Stevens  
*Résilience et capacité de survie :  
 un regard sur les fenêtres de  
 vulnérabilité*

1958 afin de soutenir la recherche et le développement technologiques dans la foulée de la panique occasionnée par le lancement russe de Spoutnik<sup>7</sup>.

En 1967, alors qu'il œuvrait comme ingénieur au sein de l'ARPA, Lawrence Roberts a découvert le travail de Boehm et Baran dans les dossiers des forces aériennes<sup>8</sup>. L'ARPA a fini par adopter la commutation de paquets dans la première version d'Internet (la bien nommée ARPANET)<sup>9</sup>. En 1969, des équipes de recherche de l'Université Stanford et de UCLA ont tenté de communiquer entre elles pour la première fois à l'aide d'ordinateurs. Au cours de cette tentative notoire, seules les lettres L et O du message « login » ont pu être envoyées avant que la connexion ne s'interrompe au milieu de l'opération<sup>10</sup>.

La version actuelle d'Internet emploie encore aujourd'hui la méthode de la commutation de paquets, élaborée par des chercheurs comme Boehm et Baran et mise en œuvre par l'armée américaine. De nos jours, l'information numérique est encore envoyée de façon fragmentaire par l'entremise de nœuds de réseaux différents, évoquant la vigilance du gouvernement américain



11. Scott Brown, « WarGames: A Look Back at the Film That Turned Geeks and Phreaks Into Stars », *Wired*, 21 juillet 2000, <https://www.wired.com/2008/07/ff-wargames/> ; « The DEF CON Story », *DEF CON*, <https://www.defcon.org/html/links/dc-about.html>. Le terme militaire de « *wargames* », qui se retrouve dans le titre du film, est aussi un type d'entraînement utilisé aujourd'hui par les pirates informatiques. Voir Andy Greenberg, « Hurricane-Bound Hacker? Here's A Rainy Day Web-Hacking War Game », *Forbes*, 28 octobre 2012, <https://www.forbes.com/sites/andygreenberg/2012/10/29/hurricane-bound-hacker-heres-a-rainy-day-web-hacking-war-game/>.

12. Stephen Van Evera, « Offense, Defense, and the Causes of War », *International Security*, vol. 22, n° 4, 1998, p. 5-43, doi:10.2307/2539239.

Yuan Stevens

*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

face à une atteinte potentielle aux données de communication en pleine guerre froide.

D'un point de vue personnel, depuis que mes intérêts de recherche se sont tournés vers les pirates informatiques en 2015, et à partir de l'année suivante, où je suis devenue une membre active des communautés de *hackers*, j'ai constaté que certains termes aux origines militaires sont couramment employés dans le secteur de la sécurité informatique. Dès qu'on pénètre l'univers du piratage (en particulier dans le contexte nord-américain), on entend parler de l'incontournable convention de piratage DEF CON. Ce titre est à la fois un clin d'œil au film *WarGames*, sorti en 1983 et mettant en vedette un jeune Matthew Broderick interprétant un pirate informatique qui déclenche une guerre nucléaire, et au système d'alerte de l'armée américaine appelé le « *defense readiness condition* » (état de préparation de la défense)<sup>11</sup>.

Dans le secteur de la sécurité informatique, on distingue deux sortes de piratage : « défensif » (dans un but de protection) et « offensif » (axé sur l'attaque), des termes sportifs qui pourraient tout autant – et sans doute est-ce plus plausible – être issus du lexique des tactiques militaires américaines<sup>12</sup>. Les pirates emploient

13. *A Guide to Red Teaming*, Wiltshire, UK, The Development, Concepts and Doctrine Centre, Ministry of Defence, 2010, [https://www.act.nato.int/images/stories/events/2011/cde/rr\\_ukdcdc.pdf](https://www.act.nato.int/images/stories/events/2011/cde/rr_ukdcdc.pdf).

souvent des termes répandus dans le contexte militaire, tels que « menace » et « adversaire », ainsi que « *red team* » et « *blue team* », qui renvoient à une série d'exercices militaires visant à déterminer l'état de préparation du corps d'armée<sup>13</sup>.

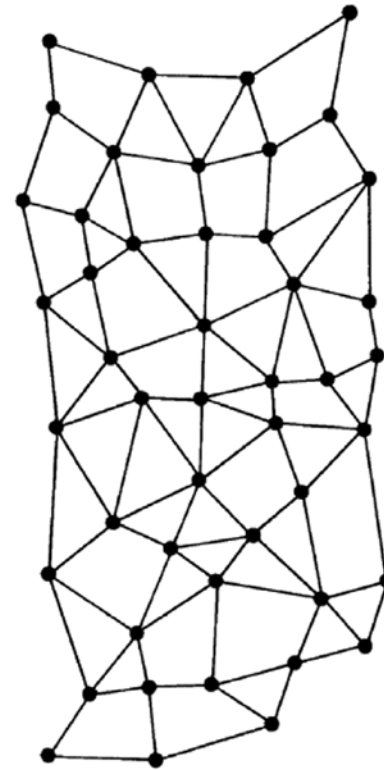


Figure 2: Réseau de communications numérique distribué de Boehm et Baran (Source : RAND Corporation Memorandum RM-3420-PR, août 1964, 2.)

Yuan Stevens  
*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*



14. Pour plus d'information sur les rapports entre la guerre froide et les origines de l'Internet, voir Benjamin Peters, *How Not to Network a Nation: The Uneasy History of the Soviet Internet*, Cambridge, Massachusetts, MIT Press, 2016. Voir aussi Rosenzweig, « Wizards, Bureaucrats, Warriors, and Hackers » pour une analyse des multiples contextes sociaux, politiques et culturels qui ont donné lieu à l'Internet, ainsi que Gabriella Coleman, *Anonymous. Hacker, activiste, faussaire, mouchard, lanceur d'alerte*, trad. par Nicolas Calvé, Montréal, Lux éditeur, 2016, p. 65 pour une analyse de la généalogie de l'influence d'ARPANET et de Usenet (surnommé « l'ARPANET du pauvre ») sur les pirates informatiques.

15. Stanford University, *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence (AI100)*, septembre 2016, [https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report-10032016fnl\\_singles.pdf](https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report-10032016fnl_singles.pdf).

Ainsi, en contribuant de près au développement d'Internet, le complexe militaire de l'époque de la guerre froide a su façonner la conception et l'infrastructure du Web. Il a également déterminé les normes culturelles des communautés de pirates informatiques qui s'efforcent de préserver ces infrastructures techniques et les données qu'elles contiennent – et qui, à l'occasion, s'y attaquent<sup>14</sup>.

#### RECONFIGURER LA VULNÉRABILITÉ

À partir des années 1990, deux événements sont survenus dans le monde de l'informatique. Tout d'abord, un immense pan de la population (et non plus seulement des institutions gouvernementales, des universités et des entreprises) a obtenu l'accès à des ordinateurs et à Internet à domicile. De plus, d'importantes avancées en matière de puissance de calcul (à partir des années 2000 et jusque dans les années 2010) ont conduit à des percées dans le domaine du stockage informatique et de la capacité de traitement, ce qui a par la suite mené à des découvertes capitales dans le secteur de la science des données<sup>15</sup>.

16. Matt Goerzen, Elizabeth Anne Watkins et Gabrielle Lim, « Entanglements and Exploits: Sociotechnical Security as an Analytic Framework », dans *9th USENIX Workshop on Free and Open Communications on the Internet (FOCI 19)*, Santa Clara, CA, USENIX Association, 2019, <https://www.usenix.org/conference/foci19/presentation/goerzen>.

17. Information Commissioner's Office (ICO), *Big Data, Artificial Intelligence, Machine Learning and Data Protection*, 2017, <https://ico.org.uk/media/for-organisations/documents/2013559/big-data-ai-ml-and-data-protection.pdf>.

18. Voir aussi Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism*, New York, NYU Press, 2018 ; Virginia Eubanks, *Automating Inequality: How High-Tech Tools Profile, Police, and Punish the Poor*, New York, St. Martin's Press, 2018 ; Ruha Benjamin, *Race After Technology: Abolitionist Tools for the New Jim Code*, Cambridge, UK, Polity Press, 2019 ; Cathy O'Neil, *Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy*, Largo, MD, Crown Books, 2016.

Nous sommes désormais entré.e.s dans une nouvelle ère, où les éléments à protéger dans le contexte informatique vont au-delà de l'accès non autorisé aux infrastructures techniques et à leurs données, ainsi que de leur potentielle destruction. La question n'est plus simplement *ce qui* est protégé, mais plutôt *qui* est protégé et *de quels types* de préjudices technologiques <sup>16</sup>?

Prenons par exemple les technologies de reconnaissance faciale. Constituant une sous-catégorie de la reconnaissance des images, ou « vision par ordinateur », les logiciels de reconnaissance faciale automatisent le processus analogique qui permet de balayer, de traiter et de reconnaître des visages humains. De tels logiciels prédictifs sont significatifs dans la mesure où ils promettent d'immenses gains en matière de vitesse, d'échelle et de volume d'analyse de données <sup>17</sup>. Mais les spécialistes soulignent sans cesse les risques associés au fait de remplacer les processus décisionnels humains par des machines, tels que l'intrusion dans la vie privée, les résultats faussés, la discrimination... et bien souvent, tout cela à la fois <sup>18</sup>. En somme, ce qui est en jeu dans l'implantation tous azimuts de logiciels prédictifs automatisés, c'est la perte de l'autodétermination informa-

19. Simone Fischer-Hübner et al., «Online Privacy: Towards Informational Self-Determination on the Internet (Dagstuhl Perspectives Workshop 11061)», *Dagstuhl Reports* n° 1, 2011, p. 1-15, [https://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman\\_v001\\_i001\\_p001\\_11061.pdf](https://drops.dagstuhl.de/opus/volltexte/2011/3205/pdf/dagman_v001_i001_p001_11061.pdf).

20. «Algorithmic Justice League – Unmasking AI harms and biases», *Algorithmic Justice League*, <https://www.ajl.org/>. Un autre groupe qui accomplit un travail semblable est le Citizens and Technology Lab à l'Université Cornell, qui analyse la modération de contenu pour assurer la sécurité des communautés web : «About Us – Citizens and Technology Lab», *Citizens and Technology Lab*, <https://citizensandtech.org/about-cat-lab/>.

21. Amy Farley, «Meet the Computer Scientist and Activist Who Got Big Tech to Stand Down», *Fast Company*, 4 août 2020, <https://www.fastcompany.com/90525023/most-creative-people-2020-joy-buolamwini>.

22. *Ibid.*

tionnelle : la capacité qu'ont les individus à contrôler la façon dont leurs données sont traitées et utilisées<sup>19</sup>.

Cependant, des organismes comme l'Algorithmic Justice League (AJL) s'efforcent d'atténuer ces dommages, et ce faisant, ils contribuent à refaçonner et à redéfinir le terme de «vulnérabilité» dans le contexte informatique<sup>20</sup>. L'étude *Gender Shades* de Joy Buolamwini et Timnit Gebru a conclu que les algorithmes d'apprentissage machine font régulièrement preuve de discrimination fondée sur le genre et sur l'origine ethnique<sup>21</sup>. Leurs recherches ont su persuader de nombreuses grandes entreprises technologiques de mettre temporairement fin à leur offre d'outils de reconnaissance faciale au début de l'année 2020, en raison des effets néfastes de ces biais<sup>22</sup>.

L'Algorithmic Justice League a annoncé en août 2020 qu'elle mettait sur pied le projet CRASH (*Community Reporting of Algorithmic System Harms*)<sup>23</sup>. Cette initiative, qui n'en est qu'à ses débuts, examine «l'idée de construire une plateforme pour mettre en œuvre certains des mécanismes de la sécurité informatique, comme les primes aux bogues, pour contrer les effets nuisibles des algorithmes<sup>24</sup>». Le modèle des primes aux bogues, une

23. Algorithmic Justice League, «Algorithmic Vulnerability Bounty Project (AVBP) brings together key stakeholders for discovery, scoping, & iterative prototyping of tools to enable broader participation in the creation of more accountable, equitable, & less harmful AI systems», Facebook, 16 août 2020, <https://www.facebook.com/AJLUnited/photos/a.1474428859462817/2627838134121878/>.

24. «The Coded Gaze: Unpacking Biases in Algorithms That Perpetuate Inequity», *The Rockefeller Foundation* (blog), 16 décembre 2020, <https://www.rockefellerfoundation.org/case-study/unpacking-biases-in-algorithms-that-perpetuate-inequity/>.

25. Sasha Costanza-Chock, *Design Justice: Community-Led Practices to Build the Worlds We Need*, Cambridge, Massachusetts, MIT Press, 2020.

forme d’assurance-qualité participative, consiste à rémunérer des individus (donc des personnes ne travaillant pas au sein d’une organisation) lorsqu’ils rapportent des zones de vulnérabilité légitimes pouvant affecter le rendement financier d’une entreprise. En invitant les gens à déclarer des occurrences d’activité algorithmique néfaste – que ce soit une prédiction erronée menant à une arrestation, par exemple, ou encore un mauvais diagnostic médical –, la communauté AJL agit au nom de ce que l’une de ses principales membres, Sasha Costanza-Chock, appelle la «justice de design<sup>25</sup>», tout en ancrant l’autodétermination informationnelle dans la notion de «vulnérabilité».

Le programme CRASH vise à permettre à des communautés qui sont le plus à risque d’être durement touchées par les avancées technologiques d’exiger une conception véritablement participative et citoyenne des systèmes prédictifs automatisés. Pour ce faire, l’AJL exploite une faiblesse importante de la culture de la conception logicielle : le fait que les entreprises mettent souvent leurs produits et services sur le marché le plus rapidement possible, reléguant les défauts et les bogues – que ce soit sur le plan technique ou du point de vue



26. Ashkan Soltani, « Abusability Testing: Considering the Ways Your Technology Might Be Used for Harm », dans *Enigma* 2019, Burlingame, CA, USENIX Association, 2019, <https://www.usenix.org/node/226468>.

Yuan Stevens

*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

du design – à des ajustements ultérieurs<sup>26</sup>. Toutefois, il importe également d'envisager d'autres vulnérabilités potentielles qui découleraient de l'utilisation du modèle des primes aux bogues par des individus ou des entreprises. De plus amples études doivent être menées sur l'efficacité de l'assurance-qualité collaborative, ses conséquences sur les personnes qui y contribuent et la façon dont les organisations doivent réagir aux failles qui leur sont signalées.

Quoi qu'il en soit, l'Algorithmic Justice League détermine qui doit être protégé.e des effets néfastes de la technologie, et quels préjudices doivent être contrés. En donnant aux individus la capacité de découvrir une grande variété de failles (y compris des atteintes à la vie privée, des inexactitudes et des cas de discrimination), des projets comme CRASH priorisent la sécurité et le bien-être de certaines communautés vulnérables au détriment de la sécurité des données et de l'infrastructure qui les renferme.

27. Pavel Podvig, «The Window of Vulnerability That Wasn't: Soviet Military Buildup in the 1970s: A Research Note», *International Security* 33, n° 1, 2008, p. 118-138.

28. «Internet Survivability and Resilience», *Royal United Services Institute (RUSI)*, 13 novembre 2007, <https://rusi.org/publication/internet-survivability-and-resilience>.

Yuan Stevens

*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

## DE NOUVELLES PLUMES DANS LE GRAND RÉCIT

En retraçant le récit des ordinateurs interreliés tels que nous les connaissons aujourd'hui, il devient plus facile de comprendre l'évolution du terme informatique de «vulnérabilité». Les architectes d'Internet, dans le contexte de la guerre froide et des craintes liées à la montée de la menace nucléaire, ont façonné le design du Web et des objets qui y sont associés – notamment l'infrastructure de communication gouvernementale ainsi que ses données –, conçus comme vulnérables et dignes de protection contre l'intrusion étrangère. Pour employer une autre expression datant de la guerre froide qui a été récupérée par le jargon des pirates informatiques, Internet a été créé dans une *fenêtre de vulnérabilité* bien précise<sup>27</sup>. Ainsi, la capacité de survie et la résilience des systèmes militaires américains se trouvent à l'origine de la mission d'Internet<sup>28</sup>.

Toutefois, un changement s'est opéré dans notre compréhension de ce qui constitue une vulnérabilité, et ceux et celles à qui revient la décision ne sont plus les mêmes qu'auparavant. Devant la prolifération de tech-



nologies prédictives et les risques qu'elles représentent, des groupes comme l'Algorithmic Justice League reprennent à leur compte la logique du secteur de la sécurité informatique. Ils permettent ainsi aux communautés les plus marginalisées de pallier leur manque d'autodétermination informationnelle et de subvenir à leurs propres besoins de survie et de résilience, qu'ils méritent désormais de combler dans le grand récit du développement technologique.

— Traduit de l'anglais par Luba Markovskaia

Yuan Stevens  
*Résilience et capacité de survie :  
un regard sur les fenêtres de  
vulnérabilité*

YUAN (rime avec Suzanne) STEVENS est une chercheuse axée sur l'action concrète qui œuvre au carrefour du droit, des politiques publiques et de la sécurité informatique. Son travail permet à la société de comprendre et de pallier les vulnérabilités aux atteintes nuisibles dans les systèmes sociotechniques et légaux. Elle a obtenu son B.C.L./JD de l'Université McGill en 2017, où elle a travaillé à titre d'assistante de recherche auprès de Gabriella Coleman, spécialiste en piratage informatique. Stevens siège au comité directeur de l'Open Privacy Research Society et est chercheuse affiliée au Data & Society Research Institute.

Elizabeth Vander Zaag  
*Digit Reproduces  
Digit and Man  
Through the Holes*

Les oeuvres sont disponibles en diffusion vidéo jusqu'au 8 août 2021. Après cette date il est possible d'obtenir un accès de visionnement temporaire en communiquant avec la Galerie à l'adresse suivante [ellen.artgallery@concordia.ca](mailto:ellen.artgallery@concordia.ca)

## TERMES



Elizabeth Vander Zaag

*Digit Reproduces*, 1978.

Vidéo animée par ordinateur, couleur, anglais, 1 min 25 s

*Digit and Man*, 1980.

Vidéo, couleur, anglais, 2 min 48 s

*Through the Holes*, 1981.

Vidéo, couleur, anglais, 3 min 30 s

Anne-Marie Trépanier

« *An infinity of solutions* ».

*Tactiques de résilience  
technologique dans les  
vidéos d'Elizabeth  
Vander Zaag*



Penser la pratique d'Elizabeth Vander Zaag à travers le prisme de la vulnérabilité, tout particulièrement celle causée par la *mise en données* des corps, c'est d'abord constater les méthodes déployées par l'artiste médiatique afin de mettre en échec l'abstraction logique popularisée par la cybernétique. C'est également penser comment sa démarche fait preuve de résilience et d'une ouverture radicale aux risques en expérimentant avec les techniques numériques et en profanant leurs fonctions prescrites.

Les trois courtes vidéos qui composent le présent corpus ont toutes en commun l'emploi de stratégies ciblées – l'accès aux ressources, les usages obliques des médias et l'incarnation du numérique – qui éveillent un potentiel de recherche créatif et artistique occulté par les usages traditionnels des médias. Tirées de la série de monobandes *Digit* (1977-1980), les vidéos *Digit Reproduces* (1978) et *Digit and Man* (1980) mettent en scène un personnage féminin dénommé Digit qui traverse diverses péripéties numériques. Diffusée lors du programme télévisé *The Gina Show*, une émission expérimentale produite par des artistes et mise en onde sur le canal public Vancouver Cable 10, cette série

Anne-Marie Trépanier  
« *An infinity of solutions* ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*

prend d'assaut l'espace télévisuel saturé de productions commerciales pour y insuffler un peu de sa satire médiatique. La monobande *Through the Holes* (1981), quant à elle, examine de près des images au petit écran à l'aide d'un objectif macro. Les trois vidéos se déploient sur fond de musique électronique rythmée et de narrations parfois chantées par l'artiste, qui nous guident à travers les compositions visuelles.

#### OUVRIR L'ACCÈS

En s'introduisant à l'intérieur de différents systèmes académiques, artistiques, numériques, Vander Zaag se joue de la *restriction d'accès* centrale à la sécurité informatique. Comme plusieurs de ses pairs artistes qui occupent des rôles de techniciennes, secrétaires, ou assistantes de production<sup>1</sup>, elle tire profit de ses activités professionnelles et des accès privilégiés qu'elles lui donnent afin de développer ses expérimentations formelles. Vers la fin des années 70, son intérêt pour l'informatique gagne de l'ampleur alors qu'elle étudie les arts informatiques et travaille comme technicienne vidéo pour la CBC et au centre Western Front<sup>2</sup>, ainsi

1. Il est particulièrement intéressant de constater les similitudes de parcours chez plusieurs femmes vidéastes canadiennes dans le survol offert par Lisa Steele dans «Committed to Memory: Women's Video Art Production in Canada and Quebec», dans *Work in Progress: Building Feminist Culture*, Rhea Tregebov (dir.), Toronto, Women's Press, 1987, p. 39-63.

2. Vander Zaag est également fermement impliquée dans la communauté d'art vidéo de Vancouver auprès des centres d'artistes auto-gérés Pumps Gallery et Video In.

Anne-Marie Trépanier  
«*An infinity of solutions*». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*



qu'à l'Université Simon Fraser (SFU) où elle accède à différents terminaux connectés aux ordinateurs centraux du campus<sup>3</sup>.

S'autorisant à expérimenter avec les moyens de production à portée de main et distribuant les savoir-faire qu'elle acquiert, notamment par la publication d'articles techniques dans la revue *Video Guide*, Vander Zaag participe à la démocratisation de l'informatique et à la littératie numérique auprès de sa communauté d'artistes vidéo. Les ressources humaines et l'équipement disponibles à la SFU, notamment le Evans & Sutherland Picture System du département de kinésiologie ainsi que les systèmes de traitement numérique du département d'audiovisuel et du Sonic Research Studio, alors géré par le compositeur électroacoustique Barry Truax, contribuent à l'élaboration de compositions hybrides croisant art vidéo et médias numériques<sup>4</sup>. Or, sa position en tant qu'artiste lui permet de se dissocier de la rigueur académique afin d'aborder la création numérique dans une approche critique, mais enthousiaste.

3. Fondation Daniel Langlois pour l'art, la science et la technologie, « Elizabeth Vander Zaag », 2001, <https://www.fondation-langlois.org/html/e/page.php?NumPage=256>; Katharine Stein, « Creative Metamorphoses : Early Experimentation with Digital Technology in the Works of Sarah Jackson and Elizabeth Vander Zaag », Mémoire de maîtrise, Université Concordia, 2019, p. 7.

4. Stein, « Creative Metamorphoses », p. 7-8.

Anne-Marie Trépanier  
« *An infinity of solutions* ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*

EXPÉRIMENTATION, USAGES OBLIQUES ET PERVERSION  
DU TECHNOLOGIQUEMENT CORRECT

Les pratiques médiatiques déviantes qui pervertissent les usages dits « technologiquement corrects<sup>5</sup> » trouvent leur force dans l'affirmation de leur partialité plutôt que dans leur pouvoir de persuasion. Elles nous invitent à adopter un point de vue transversal et à envisager la technologie dans son inévitabilité plutôt que dans son caractère innovant. Ces pratiques reconnaissent et embrassent les limitations techniques de chaque outil sans s'arrêter à un quelconque déterminisme technologique, selon lequel l'usage serait ordonné par la technologie. Au contraire, la perversion des usages technologiquement corrects met en évidence les inflexions mutuelles de la technologie et de ses utilisateur.trice.s.

Le rôle de Vander Zaag dans les différentes institutions où elle est impliquée, par exemple, lui permet de mettre à l'essai d'autres outils de production et de tester leurs potentiels comme moyens de création. En collaboration avec des scientifiques du laboratoire de kinésiologie de la SFU, elle se consacre d'une part à la numérisation du mouvement humain et récupère de l'autre

5. Dans cet article publié dans la revue *Leonardo*, l'artiste médiatique canado-mexicain Rafael Lozano Hemmer réemploie le concept du « technologiquement correct » développé par le critique d'art Lorne Falk afin de présenter comment les archétypes de l'art pionnier et de l'« avant-garde » se voient ressuscités par l'usage de la technologie comme génératrice de puissance et d'innovation. L'auteur se sert de cet article pour revaloriser les pratiques médiatiques féministes, décoloniales et minorisées qui mettent en œuvre la technologie de manière incisive et satirique, pervertissant du même coup leurs usages artistiques technologiquement corrects. Rafael Lozano-Hemmer, « Perverting Technological Correctness », *Leonardo* 29, n°1, 1996, p. 5. <https://doi.org/10.2307/1576269>.

Anne-Marie Trépanier  
« *An infinity of solutions* ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*

ces mêmes programmes pour créer son propre univers narratif autour du personnage de Digit, en réponse à l'obsession de la culture numérique pour la reproduction du réel<sup>6</sup>.

Outre le détournement de programmes de représentation graphique, l'artiste fait preuve de résilience afin d'exprimer par la voie artistique ses considérations sur l'informatique. Lorsque les portes du laboratoire se ferment, un point d'entrée s'ouvre ailleurs. Elle *fait avec* la contrainte, comme en témoigne *Digit and Man*, tournée lors d'une semaine où l'artiste n'avait pas accès aux ordinateurs de l'université, ou *Through the Holes*, où elle se retourne vers des procédés vidéos analogiques. Dans cette dernière vidéo, l'usage combiné de l'objectif macro pointé vers l'écran renverse notre position en tant que consommateur.trice.s d'images pour nous poser cette question : qu'est-ce que je regarde ? que tente-t-on de dissimuler derrière cette composition ? Les agrandissements d'écran désagrègent le flux visuel en filaments colorés, tissés plus ou moins serrés, derrière lequel on discerne un vide, une absence d'information. Ils donnent à voir la matérialité de l'image télévisée, nous incitent à regarder « par les trous », là où l'on ne devrait

6. Stein, « Creative Metamorphoses », p. 14.

Anne-Marie Trépanier  
« An infinity of solutions ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*

pas foutre son nez. À en entendre les soupirs extasiés de la narratrice, débusquer l'illusion portée par le contenu à l'écran pourrait nous apporter la jubilation d'une nouvelle liberté. *Une simulation du réel n'en demeure pas moins une réelle simulation.*

Ces réponses à l'usage technologiquement correct de l'informatique substituent la dépendance à un média ou à une technique donnée, au profit de modes discursifs libérés de toute exigence technique ou formelle. L'emploi oblique que fait l'artiste des médias numériques – ou usages *queers*<sup>7</sup> pour reprendre les mots de Sara Ahmed – infléchit l'emploi imposé, ou prescrit, afin de dégager des potentiels sous-jacents, inexploités, qui se seraient sédimentés dans la norme.

#### « VISCÉRALISER » L'INCERTITUDE

Digit est une *jeune fille en chantier*<sup>8</sup>, qui vient court-circuiter l'univers à dominance masculine de l'industrie informatique. Ce personnage imaginé par Vander Zaag est une appropriation satirique de Gidget, une série télévisée mettant en vedette une jeune adolescente affectueuse et déboussolée en quête d'amour sur les plages de Malibu.

7. La traduction de Romain Emma-Rose Bigé alterne entre les expressions « usage queer » et « usage oblique » pour décrire le concept de « *queer use* » développé par Sara Ahmed dans « Vandalisme Queer », traduit par Romain Emma-Rose Bigé, *Trou Noir* 8, 28 octobre, 2020, <https://trounoir.org/?Vandalisme-Queer-77>.

8. Traduction libre de l'expression « a wench in the works » employée par Sarah Franklin et citée par Sara Ahmed dans « Queer Vandalism », *feministkilljoys* (blogue), 9 octobre 2019, <https://feministkilljoys.com/2019/10/09/queer-vandalism/>.

Anne-Marie Trépanier  
« *An infinity of solutions* ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*



Bien que Digit soit née-numérique, elle traverse des expériences analogues à sa consœur humaine : bravant sa timidité, elle s'adonne à des aventures romantiques avec différents périphériques. Les activités reproductives de Digit sont d'ailleurs source d'angoisse pour Data et Mama, qui souhaitent protéger leur enfant en employant un.e agent.e de saisie des données.

Durant les années 40, l'ordinateur – ou plutôt, l'ordinateuse – était le plus souvent une femme, employée à exercer les commandes énoncées par un.e opératrice. Considérées comme intrinsèquement aptes à exercer ces tâches de maintenance, les premières programmeuses ont joué un rôle crucial dans le développement des technologies informatiques<sup>9</sup>. Or, les procédés d'abstraction associés au développement des langages informatiques et de la scission de la machine en deux parties distinctes – le logiciel et le matériel – ont eu pour conséquence d'invisibiliser le travail des femmes en programmation<sup>10</sup>. Dans la série *Digit*, la jeune fille ne se trouve plus à l'extérieur de l'ordinateur central, à brancher des câbles et à entrer des commandes manuellement dans le système informatique ; elle s'est matériali-

9. Wendy Hui Kyong Chun, « On Software, or the Persistence of Visual Knowledge », *Grey Room* 18, janvier 2005, p. 32-33, <https://doi.org/10.1162/1526381043320741>. À ce titre, les revues historiques des chercheuses féministes Wendy Chun, Lisa Nakamura et Sadie Plant nous ont permis de recouvrer la contribution des femmes, et particulièrement des femmes racisées, au développement de l'électronique et des technologies informatiques. En complément de la référence précédente, voir Lisa Nakamura, « Indigenous Circuits: Navajo Women and the Racialization of Early Electronic Manufacture », *American Quarterly* 66, n° 4, 2014, p. 919-941 ; Sadie Plant, *Zeros and Ones: Digital Women and the New Technoculture*, Londres, Fourth Estate, 1997.

10. Les termes « logiciel » et « matériel » sont traduits de l'anglais « *software* » et « *hardware* ». Chun, « On Software », p. 26-51.

sée à l'intérieur du processeur où elle explore elle-même, et en elle-même, les limites de son pouvoir d'action.

L'identité de Vander Zaag se profile sous les agglomérats de 0/1 et d'opérateurs booléens (and/or) qui composent Digit. Le processus de logique binaire sur lequel repose l'informatique se trouve au cœur de *Digit and Man*, où Vander Zaag s'adonne à un exposé parodié sur les différences et les ressemblances entre Digit et l'homme. Dans la vidéo, les rôles joués par les protagonistes se fondent l'un dans l'autre. L'artiste s'expose à l'écran à la fois dans le rôle de Digit, dans une série de pauses déconcertantes, une chorégraphie aux allures plutôt aléatoires et improvisées, puis d'une narratrice à l'air sérieux, dont l'exposé lui concède une autorité sur ce qui se déroule à l'écran. Ces nombreux brouillements confirment que Digit n'est pas qu'une simple numérisation de l'artiste, mais plutôt une *extension d'elle-même*, pour reprendre quelques mots presque trop célèbres de McLuhan. Et cette extension n'est pas purement technique, elle est sensible aux affects de sa protagoniste dans l'espace numérique par la médiation de l'ordinateur. Énumérant une séquence interminable de cause à effets, la protagoniste exécute des mouvements

Anne-Marie Trépanier  
« An infinity of solutions ». *Tactiques  
de résilience technologique dans  
les vidéos d'Elizabeth Vander Zaag*



hésitants, comme si elle cherchait une réponse dans sa mémoire interne : OUI, NON, OUI ET/OU NON ? Qu'advient-il en cas d'indécision ? Doit-il toujours y avoir une réponse préprogrammée ?

Le recours aux tactiques exposées précédemment, soit la démocratisation des ressources, les usages marginaux des médias et la critique des paradigmes technologiques dominants, sert à appuyer l'agentivité de Vander Zaag dans le développement de sa démarche. Plutôt que de se laisser encombrer par l'exactitude technique, son travail démontre une ouverture radicale aux potentialités inexplorées des technologies numériques et fait fi des protocoles pour raviver le plaisir ressenti lorsque l'on se donne le champ libre. Chercher les possibles, accueillir la vulnérabilité, c'est se risquer à l'échec : mais entre les deux se trouve une infinité de pistes qui ouvrent la voie vers l'expérimentation.

ANNE-MARIE TRÉPANIÉRIER est artiste, chercheuse et travailleuse culturelle. Informée par la critique féministe et queer des médias et de la technologie, ses recherches et sa pratique se concentrent sur les infrastructures alternatives de l'information et les économies de soins en relation avec les technologies numériques. Avec sa complice Laure Bourgault, elle co-dirige *Cigale*, une revue bilingue d'écrits d'artistes contemporain.e.s. Trépanier poursuit présentement des études de maîtrise en Media Studies à l'Université Concordia.

Anne-Marie Trépanier  
« *An infinity of solutions* ». *Tactiques de résilience technologique dans les vidéos d'Elizabeth Vander Zaag*

TERMES  
VULNÉRABILITÉ – VOLET 2  
HIVER 2021

Élaboré par  
Julia Eilers Smith,  
Robin Simpson,  
Michèle Thériault

Commissaire, volet 2 :  
Julia Eilers Smith

Essais :  
Yuan Stevens,  
Anne-Marie Trépanier

Oeuvres :  
Elizabeth Vander Zaag

Révision :  
Julia Eilers Smith,  
Michèle Thériault

Traduction :  
Luba Markovskaia

Distribution des vidéos :  
Vtape

Design :  
Karine Cossette

Publication disponible en version  
numérique et imprimée

© Yuan Stevens,  
Anne-Marie Trépanier,  
Galerie Leonard & Bina Ellen /  
Université Concordia

Dépôt légal  
Bibliothèque et Archives  
nationales du Québec  
Bibliothèque et Archives Canada, 2021  
ISBN 978-2-924316-27-6

[ellengallery.concordia.ca](http://ellengallery.concordia.ca)

Comment un terme circule-t-il en société, et comment sa dissémination dans le discours contemporain nous renseigne-t-elle sur la manière dont cette société se pense ? De quelles façons certains mots s'installent-ils de manière récurrente dans le langage et la sphère publique au point de devenir des lieux communs ? *Termes* est un programme discursif et artistique en ligne qui cherche à déplier, un à la fois, des termes englobants et polysémiques couramment employés dans la société contemporaine pour aborder des problématiques sociopolitiques diverses. Si certains

termes acquièrent, au fur et à mesure de leurs usages, de multiples acceptions, ils tendent souvent à se généraliser, risquant au fil de leur évolution de voir leurs sens se diluer, devenir confus ou difficile à cerner. Leur persistance dans notre vocabulaire requiert toutefois qu'on s'y s'attarde avec attention, qu'on les analyse du point de vue de leur valeur étymologique, densité sémantique ainsi que de leur circulation par-delà les frontières disciplinaires.

Pour chaque terme déployé, un.e chercheur.e invité.e en dehors du champ des arts visuels entreprend, à travers la publication d'un

texte, de l'examiner dans ses variantes, ses tensions et ses ambiguïtés sous l'angle précis de son domaine d'activité. Ce vocable est ensuite envisagé dans sa rencontre avec une œuvre sélectionnée diffusée sur le site web de la Galerie. Puis, cette œuvre sert à son tour de point de départ à l'écriture d'un second texte issu du champ culturel qui s'alimente à même le premier texte et hors de lui, afin de sonder des aspects du terme dans ses multiples occurrences.

