TERMS

PART 2

WINTER 2021

Vulnerability

Yuan Stevens
Survivability and Resilience: A View into Windows of Vulnerabilities

1. Sharla P. Boehm and 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.

2. Stewart Brand, "Founding Father," *Wired*, March 1, 2001, https://www.wired.com/2001/03/baran/.

Yuan Stevens
Survivability and Resilience: A View into Windows of Vulnerabilities

Implicit in the computing term "vulnerability" lies the assumption that computer systems and the data they contain are the objects that deserve protection from intrusion. Yet analysis of the term's meaning over time shows a rich and storied past and future, with important implications for populations deemed vulnerable.

CONFIGURING VULNERABILITY

Perhaps the first mention of the term vulnerability in the context of modern computing occurred in the 1960s. Writing for the US military think tank RAND, Sharla Boehm and Paul Baran were exploring solutions to ensure the survival and resilience of the US Air Force's communications systems at the height of the Cold War. In their seminal paper from 1964, the two computer scientists proposed a radical, decentralized model for the sharing of communications data.[1]

At the time, communications systems transferred message data from one location to another using analogue technology where transfer was full and immediate.[2] Yet in an earlier report, Baran (relying on the work of Boehm, née Perrine) stated that a nuclear attack

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.

4. Ibid., 7.

Yuan Stevens
Survivability and Resilience: A View into Windows of Vulnerabilities

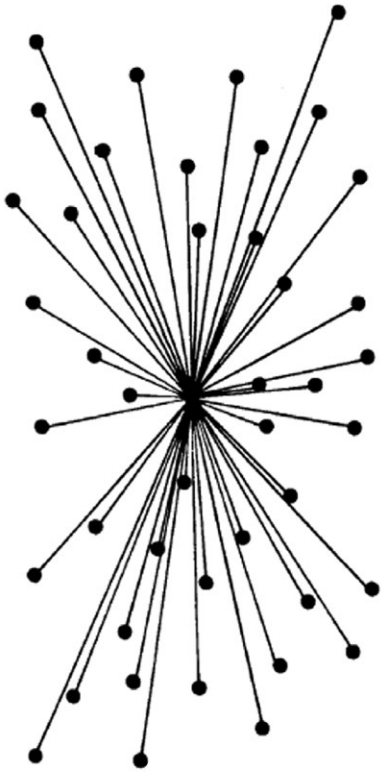

Figure 1: Boehm and Baran's centralized, analogue communications network (Source: RAND Corporation Memorandum RM-3420-PR, August 1964, 2).

could destroy the analogue communications system then in use around the globe—erasing messages en route to their destination.[3]

Baran believed that the US government's infrastructure was critically in need of preservation. "[A distributed] system," he wrote, "would do much to help preserve our democratic institutions after a possible nuclear attack."[4] Boehm and Baran's proposal was an

5. Ibid.

6. Boehm and Baran, *On Distributed Communications*; Roy Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers: Writing the History of the Internet," *The American Historical Review* 103, no. 5 (1998): 1530-552, doi:10.2307/2649970.

7. Ibid.

8. Ibid.

9. Ibid.

effort to "minimize vulnerability"[5] in the Cold War context, where the object of protection was US government infrastructure.

Boehm and Baran's solution identified the benefits of what we now call "packet switching."[6] Understood simply, the centralized, analogue system shares a whole book at once. In contrast, the distributed digital model shares pages (i.e., packets of data) over time, which are pieced together at the end destination. Packet switching safeguards against complete destruction of information that has been transferred while in transit.

In the late 1960s, the US military finally implemented Boehm and Baran's work. The US Department of Defense decided to build its own new communications network, and founded the Advanced Research Projects Agency (ARPA) in 1958 to support tech research and development in the panicked wake of Russia's launch of Sputnik.[7]

An engineer working for ARPA, Lawrence Roberts, discovered Boehm and Baran's work in the US Air Force files in 1967.[8] ARPA ultimately implemented packet switching in the first version of the internet (aptly dubbed ARPANET).[9] In 1969, research teams at

10. Rosenzweig, «Wizards, Bureaucrats, Warriors, and Hackers,»1530-552; Claire L. Evans, *Broad Band: The Untold Story of the Women Who Made the Internet* (New York: Portfolio/Penguin, 2018), 179.

Yuan Stevens
Survivability and Resilience: A View into Windows of Vulnerabilities

Stanford University and UCLA attempted to communicate with each other for the first time using computers; only the letters L and O out of the message "login" were sent before the connection infamously crashed partway through.[10]

What we now call the internet utilizes, to this day, the design feature of packet switching, pioneered by researchers such as Boehm and Baran and operationalized by the US military. Digital information is still sent in small chunks across multiple networked nodes, drawing back to a particular conception of possible harm for communications data that so prominently appeared to exist for the US government in the Cold War era.

On a personal note, since turning my academic gaze towards computer hackers in 2015 and actively participating in hacker communities since 2016, I have learned that certain terms with military origins are used across the board in the computer security industry. Enter the hacking world (especially in the North American context) and you quickly learn about the landmark hacker conference DEF CON—a term that acts as a head nod to both the 1983 film *WarGames* (featuring a young Matthew Broderick as a hacker who sets off a nuclear

11. Scott Brown, "WarGames: A Look Back at the Film That Turned Geeks and Phreaks Into Stars," *Wired*, July 21, 2000, https://www.wired.com/2008/07/ff-wargames/; "The DEF CON Story", *DEF CON*, https://www.defcon.org/html/links/dc-about.html. The military term "wargames," the film's namesake, is also a type of training exercise now used by computer hackers. See Andy Greenberg, "Hurricane-Bound Hacker? Here's A Rainy Day Web-Hacking War Game," *Forbes*, October 29, 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* 22, no. 4 (1998): 5-43, doi:10.2307/2539239.

war) as well as the US military's alert system called the "defense readiness condition."[11]

People in the computer security industry also distinguish between "defensive" (or protective) and "offensive" (or attack-oriented) hacking, two terms often used in sports that could just as easily and far more likely find their origin in the tactics of US military strategies.[12]

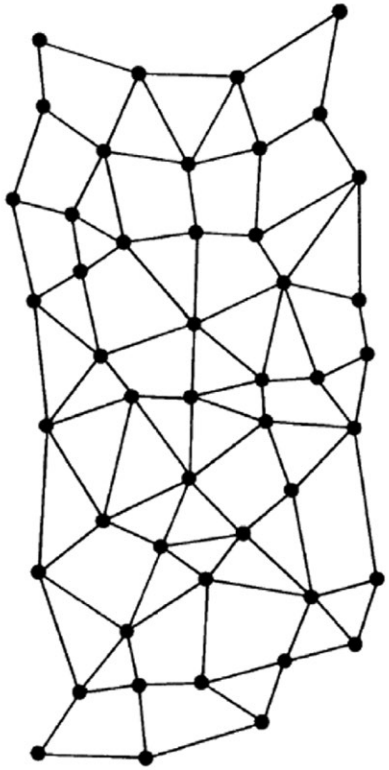

Figure 2: Boehm and Baran's distributed, digital communications network (Source: RAND Corporation Memorandum RM-3420-PR, August 1964, 2).

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.

14. For more information on the relationship between the Cold War and the origins of the internet, see Benjamin Peters, *How Not to Network a Nation: The Uneasy History of the Soviet Internet* (Cambridge, Massachusetts: MIT Press, 2016). See also Rosenzweig, "Wizards, Bureaucrats, Warriors, and Hackers" for analysis of the multiple social, political and cultural contexts in which the internet came to be, as well as Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces Of Anonymous* (Brooklyn, NY: Verso books, 2014): 65 for analysis of the genealogy and impact of ARPANET and Usenet (dubbed 'the poor man's ARPANET') on computer hackers.

Hackers routinely use terms that figure prominently in the military context such as "threat" and "adversary" as well as "red team" and "blue team," the latter two which allude to a set of exercises used by the military to identify task force readiness.[13]

With this in mind, through intimate involvement in the internet's development, the Cold War military complex has come to greatly shape the design and infrastructure of the internet, as well as the cultural norms of the hacker communities who work to protect (and at times harm) such technical infrastructure and the data it contains.[14]

RECONFIGURING VULNERABILITY

By the 1990s and beyond, two things occurred in the world of computing. First, a huge swathe of households (and not just government institutions, universities and corporations) gained access to computers and the internet. Second, significant advances in computing power (starting in the 2000s and continuing into the 2010s) led to breakthroughs in computer storage and processing

15. Stanford University, *Artificial Intelligence and Life in 2030: One Hundred Year Study on Artificial Intelligence* (AI100) (September 2016), https://ai100.stanford.edu/sites/g/files/sbiybj9861/f/ai100report10032016fnl_singles.pdf.

16. Matt Goerzen, Elizabeth Anne Watkins and Gabrielle Lim, "Entanglements and Exploits: Sociotechnical Security as an Analytic Framework," in *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. See e.g. Safiya Umoja Noble, *Algorithms of Oppression: How Search Engines Reinforce Racism* (New York: NYU Press, 2018); Virginia

power, in turn leading to huge breakthroughs in data science.[15]

We now find ourselves in a new era where the objects of protection in the context of computing have expanded beyond unauthorized access to—and potential destruction of—technical infrastructure and its data: the question can no longer be *what* is protected, but must include *who* is protected and from *what kind* of harms made possible by technology?[16]

Consider face recognition technology. A subset of image recognition or computer vision, face recognition software automates the analogue process of scanning, identifying and recognizing (human) faces. Such predictive software is significant for the way it promises huge gains in the speed, scale, and volume of data analysis it provides.[17] But experts continue to highlight the risks that come when we replace human decision-making processes—such as intrusion into our private lives, inaccurate findings, discrimination, and often all of the above at the same time.[18] In sum, at stake in the unfettered implementation of automated, predictive software is the loss of informational self-determination—the

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).

19. Simone Fischer-Hübner et al., "Online Privacy: Towards Informational Self-Determination on the Internet (Dagstuhl Perspectives Workshop 11061)," *Dagstuhl Reports* 1 (2011): 1-15, 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/. Another group doing similar work includes the Citizens and Technology Lab at Cornell University, which analyzes content moderation practices for safer online communities: "About

ability for individuals to control how their data is used and processed.[19]

But organizations like the Algorithmic Justice League (AJL) are working to mitigate these harms, and in doing so, are helping to reconfigure and redefine our conception of the term "vulnerability" in the context of computing.[20] Joy Buolamwini and Timnit Gebru's *Gender Shades* study has identified that machine learning algorithms routinely discriminate on the basis of gender and race.[21] Their research helped to persuade numerous prominent tech companies to temporarily cease offering their face recognition software in early 2020, due to the harms engendered by such bias.[22]

The Algorithmic Justice League announced in August 2020 what is now called the CRASH (*Community Reporting of Algorithmic System Harms)* project.[23] The endeavour, while still in its early stages, is exploring "the idea of building a platform to apply some of the information security models, like bug bounties, to the algorithmic harms space."[24] The bug bounty model of crowdsourced quality assurance pays individuals (working outside an organization) to report legitimate vulnerabilities that affect the organization's bottom line.

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*, August 4, 2020, https://www.fastcompany.com/90525023/most-creative-people-2020-joy-buolamwini.

22. Ibid.

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, August 16, 2020, https://www.facebook.com/AJLUnited/photos/a.1474428859462 817/2627838134121878/.

24. "The Coded Gaze: Unpacking Biases in Algorithms That Perpetuate Inequity," *The Rockefeller Foundation* (blog),

By inviting people to disclose instances of algorithmic harm—whether it's a wrongful prediction leading to arrest, for example, or an inaccurate medical diagnosis—the AJL community is effecting what one of its core members, Sasha Costanza-Chock, calls "design justice"[25] all while centering people's informational self-determination in the definition of "vulnerability."

The CRASH program aims to enable communities that stand to be the most detrimentally affected by technological advancement to push for the meaningful, bottom-up, participatory design of automated, predictive systems. To do this, the AJL is harnessing a major weakness of the culture of software design, where companies often release their products or services as soon as possible, rendering the software's (technical and design) flaws and harms an afterthought.[26] However, it is equally important to consider other vulnerabilities that can arise as the bug bounty model is used by organizations or taken up by individuals. More research is needed on the effectiveness of crowdsourced quality assurance, its impacts on people who contribute and how organizations ought to respond to flaws that are found.

December 16, 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).

26. Ashkan Soltani, "Abusability Testing: Considering the Ways Your Technology Might Be Used for Harm," in *Enigma 2019* (Burlingame, CA: USENIX Association, 2019), https://www.usenix.org/node/226468.

The Algorithmic Justice League is, in any case, identifying who should be protected from harm that emanates from technology and what kind of harm is worth redressing. By potentially enabling people to disclose a wide range of flaws (including privacy breaches, inaccuracy and instances of discrimination), projects like CRASH prioritize the safety, security and well-being of certain (vulnerable) communities, rather than the security of data and its enclosing infrastructure.

EMERGING AUTHORS IN THE NARRATIVE ARC

We better understand the evolution of the computing term "vulnerability" when we trace the narrative arc of interconnected computers as we know them today. The internet's architects, against the backdrop of Cold War fears related to nuclear proliferation, informed the design of the internet and the objects associated with it—namely, government communications infrastructure itself along with its data—that were deemed vulnerable and worthy of protection from intrusion. To use another Cold War phrase that has made its way into hacker

27. Pavel Podvig, "The Window of Vulnerability That Wasn't: Soviet Military Buildup in the 1970s: A Research Note," *International Security* 33, no. 1 (2008): 118–38.

28. "Internet Survivability and Resilience," *Royal United Services Institute (RUSI)*, November 13, 2007, https://rusi.org/publication/internet-survivability-and-resilience.

Yuan Stevens
Survivability and Resilience: A View into Windows of Vulnerabilities

parlance, the internet was created in a particular *window of vulnerability*,[27] thereby prioritizing the survivability and resilience of US military communications systems, one of the original purposes of the internet.[28]

But we have seen a shift in what is deemed a vulnerability, and who gets to decide. In response to the proliferation of predictive technology and the risk of its concomitant harms, groups like the Algorithmic Justice League have started to adopt the logics of the computer security industry—allowing some of the most marginalized populations to redress a lack of informational self-determination, and a need for survivability and resilience that they, too, deserve in the narrative arc of the development of technology.

YUAN (rhymes with Suzanne) STEVENS is an action-oriented researcher working at the intersections of law, policy, and computer security. Her work equips society with the ability to understand and patch up harmful vulnerabilities in sociotechnical and legal systems. She received her B.C.L./JD from McGill University in 2017, working as a research assistant for hacker expert Gabriella Coleman. She serves on the board of directors for Open Privacy Research Society and is a research affiliate with Data & Society Research Institute.

Elizabeth Vander Zaag

Digit Reproduces Digit and Man Through the Holes

The works are available for streaming until August 8, 2021. After this date you may contact the Gallery at ellen.artgallery@concordia.ca to receive a link to temporarily access the works.

Elizabeth Vander Zaag

Digit Reproduces, 1978.
Computer animated video, colour, 1 min. 25 sec.

Digit and Man, 1980.
Video, colour, 2 min. 48 sec.

Through the Holes, 1981.
Video, colour, 3 min. 30 sec.

Elizabeth Vander Zaag, *Throught the Holes*, video still, 1981. Video, colour, 3 min. 30 sec. Courtesy Vtape.

Anne-Marie Trépanier

"An Infinity of Solutions." Tactics of Technological Resilience in the Videos of Elizabeth Vander Zaag

To consider Elizabeth Vander Zaag's practice through the prism of vulnerability, particularly one brought on by the *datafication* of bodies, is to note the methods used by this media artist to thwart the logical abstraction popularized by cybernetics. It also means thinking about how her work demonstrates a radical openness to risk by experimenting with digital technologies and dismissing their prescribed functions.

The three short videos that make up this body of work each employ targeted strategies—access to resources, oblique use of media, and the embodiment of the digital—that awaken potential artistic research and creation normally eclipsed by traditional media uses. *Digit Reproduces* (1978) and *Digit and Man* (1980), two videos from her single-channel series *Digit* (1977-1980), feature a female character named Digit who experiences a variety of digital adventures. Broadcast during the TV program *The Gina Show*, an experimental program produced by artists and aired on the public channel Vancouver Cable 10, the series injected a touch of media satire into a commercially saturated televisual space. *Through the Holes* (1981) is a single-channel video that closely examines television images through a macro

Anne-Marie Trépanier

"An Infinity of Solutions." Tactics of Technological Resilience in the Videos of Elizabeth Vander Zaag

lens. The three videos play over a background of rhythmic electronic music and narratives, sometimes sung by the artist, that guide us through the visual compositions.

OPENING ACCESS

By inserting herself within different academic, artistic, and digital systems, Vander Zaag defies the *restricted access* that is central to IT security. Like many of her artist-peers who occupy roles as technicians, secretaries, or production assistants,[1] Vander Zaag uses her professional activities and access privileges to develop her formal experimentations. In the late 1970s, her interest in IT grew when she studied computer arts and worked as a video technician for the CBC, at Western Front,[2] and at Simon Fraser University (SFU), where she had access to different terminals connected to the mainframe computers on campus.[3]

By allowing herself to experiment with available resources and sharing her acquired knowledge, namely by publishing technical articles in *Video Guide* magazine, Vander Zaag helped democratize information technology and digital literacy among her community

1. It is particularly interesting to note the similarities in occupations held by many Canadian women video artists featured in Lisa Steele's survey "Committed to Memory: Women's Video Art Production in Canada and Quebec," in *Work in Progress: Building Feminist Culture*, ed. by Rhea Tregebov (Toronto: Women's Press, 1987): 39-63.

2. Vander Zaag was also deeply involved in Vancouver's video art community through artist-run centres such as Pumps Gallery and Video In.

3. The Daniel Langlois Foundation for Art, Science, and Technology, "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," Master's thesis, Concordia University, 2019, 7.

of video artists. The human resources and equipment available to her at SFU—namely the Evans & Sutherland Picture System in the Department of Kinesiology, the digital processing systems in the AV department, and the Sonic Research Studio, then-managed by electroacoustic composer Barry Truax—contributed in shaping her hybrid compositions that merge video art and digital technologies.[4] Her position as an artist also meant she could disassociate herself from academic rigor and approach digital creation critically yet passionately.

EXPERIMENTATION, OBLIQUE USAGE, AND THE PERVERSION OF *TECHNOLOGICAL CORRECTNESS*

Deviant media practices that pervert so-called "technologically correct"[5] usage find strength in the assertion of their subjectivity rather than their powers of persuasion. They invite us to adopt a cross-cutting perspective and to consider technology as something that is inevitable rather than innovative. These practices recognize and embrace the technical limitations of each tool without stopping at any technological determi-

4. Stein, "Creative Metamorphoses," 7-8.

5. In an article published in the magazine *Leonardo*, Canadian-Mexican media artist Rafael Lozano Hemmer reuses the concept of "technological correctness" developed by art critic Lorne Falk to describe how the archetypes of "avant-garde" and pioneering artists are revived by the use of technology as generator of power and innovation. Hemmer uses this article to reassert the value of feminist, decolonial, and minority media practices that use technology in incisive and satirical ways, while perverting their technologically correct artistic usage. Rafael Lozano-Hemmer, "Perverting Technological Correctness," *Leonardo* 29, no. 1 (1996): 5, https://www.jstor.org/stable/1576269?origin=crossref&seq=1.

nism, whereby usage is ordered by technology. On the contrary—the perversion of technologically correct usage highlights the mutual flexion of technology and its users.

Vander Zaag's role within the various institutions she works with allows her to experiment with different production tools and test their creative potential. Collaborating with scientists from the kinesiology lab at SFU, she devoted herself, on one hand, to the digitization of human movement, and on the other, to the integration of these same programs in the creation of her own narrative universe for the character of Digit—a response to digital culture's obsession with the reproduction of reality.[6]

In addition to subverting graphics programs, Vander Zaag shows resilience in expressing through her artworks her ideas on information technologies. When the lab shuts down, she finds opportunities elsewhere. She *works with* limitations, as demonstrated in *Digit and Man*, shot over the course of one week when the artist had no access to the university's computers, or *Through the Holes*, where she turns to analog video processes. In the latter video, a macro lens pointed toward the screen

6. Stein, "Creative Metamorphoses," 14.

Anne-Marie Trépanier
"An Infinity of Solutions." Tactics of Technological Resilience in the Videos of Elizabeth Vander Zaag

overturns our position as image consumers and makes us ask: What am I looking at? What is this image trying to hide? The blown-up screen images break down the visual flow into colourful, loosely-woven filaments behind which there is a void, an absence of information. They show the materiality of the televised image, and incite us to look "through the holes," where we shouldn't be sticking our nose. Judging by the narrator's rapturous sighs, uncovering the illusion of the screen's content could produce a sense of joyous liberation. *A simulation of the real is still a real simulation.*

These responses to the technologically correct use of computer technologies substitute our dependence on a given media or technique with discursive modes that are free of any technical or formal requirements. The artist's oblique use of digital technologies—or *queer*[7] use, in the words of Sara Ahmed—redirects their imposed or prescribed use to uncover the underlying and untapped potential that would have otherwise remained buried beneath the norm.

7. Sara Ahmed developed the concept of "queer use" in *What's the use? On the uses of use* (Durham: Duke University Press, 2019).

Digit is "a wench in the works"[8] who short-circuits the male-dominated universe of the computer industry. Vander Zaag's character is a satirical appropriation of Gidget, a television sitcom starring a boy-crazy teenage girl looking for love on the beaches of Malibu. But while Digit is a digital construct, her experiences are similar to those of her human counterpart: overcoming her shyness, she embarks on romantic adventures with various peripherals. Meanwhile Digit's reproductive activities are a source of anxiety for Data and Mama, who try to protect their child by hiring a data-collecting agent.

In the 1940s, computers were most often operated by women hired to enter a programmer's commands. The first female programmers were considered intrinsically apt to perform these types of maintenance tasks, and played a crucial role in the development of computer technologies.[9] At the same time the process of abstraction inherent to computer language development and the division of the machine into two distinct parts—software and hardware—made women's program-

8. A term used by Sarah Franklin and quoted by Sara Ahmed in "Queer Vandalism," *feministkilljoys* (blog), October 9, 2019, https://feministkilljoys.com/2019/10/09/queer-vandalism/.

9. Wendy Hui Kyong Chun, "On Software, or the Persistence of Visual Knowledge," *Grey Room* 18 (January 2005): 32-33, https://doi.org/10.1162/1526381043320741. In this regard, the historical journals of feminist researchers Wendy Chun, Lisa Nakamura, and Sadie Plant have allowed us to uncover the contribution of women, particularly of racialized women, in the development of electronics and information technologies. In addition to the previous reference, see Lisa Nakamura, "Indigenous Circuits: Navajo Women and the Racialization of Early Electronic Manufacture," *American Quarterly* 66, no. 4 (2014): 919-941; Sadie Plant, *Zeros and Ones: Digital Women and the New Technoculture* (London: Fourth Estate, 1997).

ming work virtually invisible. In the *Digit* series, the young protagonist is no longer outside the mainframe computer, connecting cables and manually inputting commands into the computer system; she has materialized inside the processor where she explores the limits of her agency both by and within herself.

Vander Zaag's identity surfaces through the mass of 0/1s and Boolean operators (and/or) that compose Digit. The process of binary logic on which computer technology is based is at the heart of *Digit and Man*, in which Vander Zaag creates a parodic exposé of the similarities and differences between Digit and "man." In the video, the protagonists' roles meld into each other. We see the artist play Digit in a series of disconcerting pauses, a somewhat random and improvised choreography, and as a serious narrator whose on-screen presence gives her an authoritative air. This blurring of elements confirms that Digit isn't just a simple digital creation by Vander Zaag, but an *extension of herself*, to paraphrase McLuhan's well-known words. This extension is not purely technical, it experiences the protagonist's emotions in the digital realm as mediated by the computer. Running through an endless sequence of cause and

Anne-Marie Trépanier

"An Infinity of Solutions." Tactics of Technological Resilience in the Videos of Elizabeth Vander Zaag

effect, the protagonist gestures hesitantly, as if searching her internal memory for an answer: YES, NO, YES AND/OR NO? What if she can't decide? Must there always be a preprogrammed response?

The use of tactics described above, namely the democratization of resources, the marginal use of media, and the critique of dominant technological paradigms, supports Vander Zaag's agency in the development of her work. Rather than being encumbered by technical exactitude, her work demonstrates a radical openness to the unexplored potential of digital technologies and ignores protocols to rekindle the joys of total freedom. Discovering what's possible and welcoming vulnerability means risking failure, but between these two is an endless number of paths that open the route to experimentation.

—Translated from French by Jo-Anne Balcaen

ANNE-MARIE TRÉPANIER is an artist, researcher and cultural worker. Informed by feminist and queer critiques of media and technology, her research and practice focus on alternative information infrastructures and economies of care in relation to digital technologies. With her accomplice Laure Bourgault, she is the co-editor of *Cigale*, a bilingual journal of contemporary artists' writings. Trépanier is currently completing a master's degree in Media Studies at Concordia University.

TERMS

VULNERABILITY – PART 2

WINTER 2021

Developed by
Julia Eilers Smith,
Robin Simpson,
Michèle Thériault

Curator, Part 2:
Julia Eilers Smith

Essays:
Yuan Stevens,
Anne-Marie Trépanier

Artworks:
Elizabeth Vander Zaag

Editing:
Julia Eilers Smith,
Michèle Thériault

Translation:
Jo-Anne Balcaen

Distribution of the videos:
Vtape

Design:
Karine Cossette

PART 2

TERMS

Publication available in digital
and printed editions

Legal Deposit
Bibliothèque et Archives
nationales du Québec
Library and Archives Canada, 2021
ISBN: 978-2-924316-28-3
ellengallery.concordia.ca

VULNERABILITY

How does a term circulate through society, and how does its dissemination within contemporary discourse inform us about the way that society thinks about itself? By what means do certain words instill themselves in language and the public sphere to the point of becoming commonplace? *Terms* is an online discursive and artistic program that individually unpacks a series of broad and polysemous terms that are employed today to address a range of sociopolitical issues in contemporary society. While some words acquire multiple definitions the more they are used, they also often tend to become generalized and run the risk of having their meaning become diluted, confused, or unclear over time. Nevertheless, their continued presence in our vocabulary requires careful attention and analysis as to their etymological value, their semantic density, and their use across and beyond disciplinary boundaries.

For each selected term, a researcher from outside the visual arts publishes a text that examines it in all its variants, tensions, and ambiguities through the specific lens of their field of activity. The word is then considered by pairing it with a designated artwork shared on the Gallery's website. In turn, a writer from the cultural sector uses this same work as the starting point for a second text that draws from the first and from beyond to probe some aspects of the term in its various dimensions.