Intermédialités
Histoire et théorie des arts, des lettres et des techniques
Intermediality
History and Theory of the Arts, Literature and Technologies

Introduction. The Mediality of Concealment: Material Practices and Symbolic Operativity

Nathalie Casemajor and Sophie Toupin

Number 32, Fall 2018

cacher
concealing

URI: https://id.erudit.org/iderudit/1058467ar
DOI: https://doi.org/10.7202/1058467ar

See table of contents

Publisher(s)

Revue intermédialités

ISSN

1920-3136 (digital)

Explore this journal

Cite this document

Casemajor, N. & Toupin, S. (2018). Introduction. The Mediality of Concealment: Material Practices and Symbolic Operativity. *Intermédialités / Intermediality*, (32). https://doi.org/10.7202/1058467ar

Article abstract

This special issue focuses on the cultural forms, technologies, and social logics of dissimulation. In this introduction, we propose a critical examination of the cultural and political entanglements of three emblematic domains of dissimulation: camouflage, steganography, and encryption. Focusing on the study of mediality, our analysis crosses the evolution of media environments and representations of these dissimulation processes to better understand their modes of legitimization and symbolic operativity.

The Mediality of Concealment: Material Practices and Symbolic Operativity

Nathalie Casemajor
Sophie Toupin

The tension between the need and desire to hide and reveal provides a decisive key to the understanding of struggles for agency. As a strategy, concealment responds to a range of needs: to protect that which is sensitive, to retain a strategic advantage, to deceive, or to avoid social disapproval or sanctions. The tactics used are equally diverse. They may include making invisible (camouflaging), obscuring (creating confusion, diverting attention, deceiving), revealing some parts in order to better hide what is essential (disguise, steganography, optical illusion), or protecting access (cryptography, censorship, and self-censorship).

¶2 This special issue of *Intermédialités/Intermediality* focuses on the cultural forms, technologies, social logics, and artistic experiments of concealment that traverse various medial environments and meaning-making practices. In what ways do the practices, art, and techniques of concealment participate in the formation of private and public spheres? What power dynamics are at work in this relationship? And to what extent do the metaphors of veiling/unveiling, encryption/decryption, visibility/invisibility, obfuscating/capturing allow us to understand the hidden dimensions of social life? In the context of a reflection on intermediality, we invited authors to think about the forms of this relationship in terms of the material and symbolic mediations that constitute them—their mediality. What are the logics of intermediality at play in concealment? How are different types of mediality combined and mobilized into activities of concealment? We selected for this issue contributions that examine the dynamic relationship between forms of concealment and forms of detection by situating them in their social, cultural, and technological contexts. The first section of this introduction frames the contributions in the special issue. In the second part, we propose a critical examination of the cultural and political entanglements of three technical domains of concealment: camouflage, steganography, and encryption.

The Intermedial Logics of Concealment

Fig. 1: Still from the film *How Not to Be Seen: A Fucking Didactic Educational .MOV File*, Ito Steyerl, 2013. HD video, single screen in architectural environment, 15 min 52 sec. Image courtesy of the Artist and Andrew Kreps Gallery, New York © *Ito Steyerl CC 4.0*.

Agency through invisibility

¶3 "Today the most important things want to remain invisible. Love is invisible. War is invisible. Capital is invisible." In the video *How Not to Be Seen: A Fucking Didactic Educational .MOV File* (2013), from which this excerpt is derived, filmmaker and media theorist Ito Steyerl proposes a reflection on the current socio-technological conditions of visual culture. The piece offers a humorous manual on how to escape visual representation and its corollary optical tracking systems in the context of data-driven environments. Combining documentary elements with fiction, the video features ninjas and characters using burqas as invisibility cloaks evolving in computer-generated architectural models. The set of tricks presented in the artwork wittingly plays on the ambiguous and reversible relationship between power and visibility: if invisibility in the public sphere can be the negative consequence of a lack of political representation, a lack of concern, or social stigma ("Lesson IV. How to become invisible by disappearing… Being female and over 50," states Steyerl's video), going without being noticed can also be the privilege of the powerful and the wealthy who can spread their influence and live behind closed doors ("Living in a gated community," in Steyerl's video). Invisibility can also be a way to reclaim agency, for example by escaping the technical means of data capture that feed

surveillance and commodification systems ("to jump into low resolution," as described in Steyerl's video). When visibility is a trap, as Foucault suggests,[1] actively working towards concealment holds potential for resistance and transformation.

¶4 More broadly, concealment can be understood as a central vector in the formation of private and public spheres. The intimate and the political coexist in the hidden dimension of social relations, in the veiled bodies that escape from sight, in the repression of affects. At the very heart of the processes of individuation and socialization, secrecy plays an essential role both in the formation of the psyche and in collective life.[2] It creates the possibility of a parallel world—that of the sacred or the occult, of politico-administrative mystery and secret societies, which form and transform according to the likelihood of their revealing. The contemporary world is criss-crossed by (apparently) contradictory logics, where hypervisibility in the media intersects with conspiracy theories and beliefs in a hidden truth, further fueled by the opacity of technological and financial infrastructures. In its most paranoiac forms, the perception of secrecy moves beyond the relationship between concealment and divulgation to imagine infinite and imperceptible forms of secrecy: "paranoiacs denounce the international plot of those who steal their secrets, their most intimate thoughts; or they declare that they have the gift of perceiving the secrets of others before they have formed," write Deleuze and Guattari.[3]

Medial forms of concealment

¶5 As a technique, concealment is the performance of a procedure, a form of intervention in the field of the perceptible and the knowable in order to induce or impede certain interpretations of reality in the observer. It involves both know-how (tactics, tricks, techniques of the body, behaviours) and knowledge of the medial capacity of forms and materials (the phenomenological qualities of shapes, colours, sounds, and radiations in the sensory spectrum). The know-how of concealment relies mainly on prediction and adaptation. Indeed, the action of concealing is doubly transitive: *something* is concealed, and it is hidden *to someone*—or possibly to oneself, in the psychoanalytical sense.

---

[1] Cited in Katrin Gattinger's article in this issue, Michel Foucault, *Surveiller et punir*, Paris, Éditions Gallimard, 1975.

[2] Georg Simmel, "The Sociology of Secrecy and of the Secret Societies," *American Journal of Sociology*, vol. 11, 1906, p. 441–498.

[3] Gilles Deleuze and Félix Guattari, *Capitalism and Schizophrenia. A Thousand Plateaus* [1987], trans. by Brian Massumi, Minneapolis, MN, University of Minnesota Press, 2005 p. 288.

¶6 Our premise is that the domain of the hidden, and the ways of (self)concealment, are constructed in synergy with the ways of perceiving, interpreting, judging, and tracking down that are specific to a given context and time. Each new concealment strategy creates an arsenal of tools for detection, which in turn generates new forms of concealment and detection. The art of disguise evolves with the advancement of technology (though at times it favours older types of technologies), but also according to the development of social norms and relations of power.

¶7 At the heart of the dynamic of mutual anticipation lies the fact that concealment and detection are deeply relational, evolving in a feedback loop between the observer and the observed. In the detective short story *The Purloined Letter* written by Edgar Allan Poe (1844),[4] detective Dupin criticizes the police for seeing "only their own ideas of ingenuity; and, in searching for anything hidden, advert only to the modes in which they would have hidden it." In his admonition to his fellow police detectives, Dupin criticizes their inability to anticipate the fact that the Minister who hid the letter had himself anticipated the reasoning of the investigators. Jumping out of the loop of their expectations, he "had resorted to the comprehensive and sagacious expedient of not attempting to conceal it at all."[5] The letter was located where the police expected the least to find it: openly visible in a card rack, hidden in plain sight.

¶8 The philosophical and cultural meanings of the relationships between concealment and truth have been much debated in scholarly circles. From the 1950s to the late 1980s, several literary theorists engaged in a theoretical dispute over the interpretation of *The Purloined Letter*. Inspired by Poe's story, Lacan drew from it in his "Seminar on *The Purloined Letter*," a reflection on truth, reality, the symbolic, and the unconscious in which he argues, with Jeffrey Mehlman, that "what is hidden is never but what is missing from its place."[6] Derrida, in *The Purveyor of Truth*, proposes a critique of Lacan by questioning the "psychoanalytic deciphering" through the metaphor of "the nakedness of hidden meaning." Equating veil, text, and fabric, he suggests that the same material simultaneously conceals and shows. This relationship between the visible surface and what Merleau-Ponty calls "the invisible

[4] Edgar Allan Poe, "The Purloined Letter," [1844], in *Edgar Allan Poe: The Ultimate Collection*, Los Angeles, Enhanced Media Publishing, 2016.

[5] *Ibid.*, p. 130.

[6] Jacques Lacan and Jeffrey Mehlman, "Seminar on 'The Purloined Letter'," *Yale French Studies*, no. 48, 1972, p. 55.

lining"[7] situates visibility in relation to a surface. The figure of the surface (and its corollary, depth) is especially useful to understand how the public display of an appearance can actively work to conceal hidden information beyond what is given to see.

¶9 The predominance of the visual realm and visual metaphors in discourses about concealment can be understood in relation to the predominance of sight as the master sense in Western contemporary societies. But the realms of smell and hearing are also invested with practices of concealment, and contemporary concealment techniques cover an ever-expanding range of materials and infrastructures, some of them imperceptible to human senses. In today's rapidly evolving media ecologies, things to be concealed are not just painted over, covered with a veil, or buried underground, but they are also inserted in network protocols, light waves, or in the DNA of living organisms. These techniques often combine different mediums, creating intermedial assemblages that enmesh living bodies into material and semiotic systems of concealment aimed at deceiving both the human senses and the technical mediums of detection.

Contributions to the issue

¶10 The contributions in this special issue address the logics of concealment from the point of view of digital media, cultural studies, cinema, photography, and literature. Some adopt a historical perspective in order to shed light on the development of these forms, while others focus on elucidating the logics, tensions, and paradoxes of the contemporary world.

¶11 The first two articles by Blaise Tsoualla and Rona Sela examine power relations in the context of neocolonial states. Tsoualla analyzes the literary production of Yodi Karone through the lens of the anagram. A pseudonym for Alain Ndongo Ndiye, Yodi Karone is a Franco-Cameroonian author living in Paris among political exiles. Tsoualla shows how Karone employs the word *goyave* (guava) as a transfiguration of *voyage* (travel) to deploy a universe where masking and unmasking are at play both in his own identity as an author and in the exercise of literary freedom in the context of African dictatorships. Rona Sela's article deals with another neocolonial context: that of Israel and its management of Palestinian photographic archives. Sela examines the ways in which Israel has enacted past, present, and future forms of colonialism by plundering Palestinian archives. Using the case study of

[7] Maurice Merleau-Ponty, *The Visible and the Invisible: Followed by Working Notes*, trans. by Alphonso Lingis, Evanston, IL, Northwestern University Press, 1968, p. 149.

photographer Chalil (Khalil) Rissas (Rassas), she shows how Israeli military has concealed Palestinian archives thereby enacting forms of repression and regimentation. As a result, the histories and identities of the Palestinians are erased and replaced by those of the occupying force.

¶12 A second series of contributions focuses on artistic practices and their material experimentation with forms of concealment. In the portfolio section of this issue—artiste invitée/Guest Artist—, artist Julie Morel shows a selection of works that follow trajectories of navigation, encryption, and deciphering in the spaces of archives and on the Web. The series *Clear, Deep, Dark* (2018) contrasts different facets of the Web, from the easily accessible surface to the deep ramifications of the network and the obscured territories of virtual private networks and Pretty Good Privacy (PGP) encryption keys. Katrin Gattinger investigates how clandestinity is an operational mode in the visual production of two artists: photographer Trevor Paglen and filmmaker Mohamed Bourouissa. Exposing objects, situations, or infrastructures that are meant to stay hidden, both artists question our contemporary regime of visibility and representation in which surveillance is both omnipresent and invisible. Karine Chevalier addresses the representation of disfigured faces (*gueules cassées*) in cinema through the lens of ethics. The cinematographic strategies she describes in the films *J'accuse* (Abel Gance, 1918 and 1938) and *La Chambre des officiers* (François Dupeyron, 2001) invite us to look beyond the masks to grasp the subjectivities of disfigured soldiers. Strategies of identification and disidentification are also at play in Sebastian Althoff's article on the *Facial Weaponization Suite* (2012) project by artist Zach Blas. Althoff argues that in the context of algorithmic governmentality, personal identification through face data capture and measure should be distinguished from logics of visibility.

¶13 A third theme addressed in this special issue concerns the contemporary evolutions of digital technologies and their impact on logics of concealment. Ksenia Ermoshina and Francesca Musiani examine end-to-end encryption tools, which feature security and privacy by letting the users "hide" different parts of their online identities. Their article is informed by extended fieldwork where they interviewed low- and high-risk participants from different regions of the world. This fieldwork enabled them to identify the types of data that need to be concealed depending on context, and how it is done. Aleksandra Kaminska investigates past and current techniques of storage such as holographs, kinegrams, and watermarks. One the one hand, these methods have increased the potential of humans to read (i.e. to see, detect, process, and assess) what is real. On the other hand, these devices have produced an environment that is largely unreadable—inaccessible—to human processing. Finally,

in "Surveillant Intimacies," Mél Hogan examines how dataveillance and state surveillance transform interpersonal relationships. Through creative vignettes, Hogan explores the impact of data mining on intimacy and personal relationships.

Mediality in Camouflage, Steganography, and Encryption

¶14 In the remainder of this essay, we explore the dynamics and entanglements of concealment and detection through the following questions: How do techniques of concealment operate on the symbolic and political level? What desires and fantasies do they carry? And how do they mediate relationships of power? In his analysis of infrastructures, anthropologist Brian Larkin[8] offers a framework that illuminates how techniques of concealment are part of wider systems of mediation that constitute subjectivities and ways to live in the world. His cultural analytics of material forms is relevant to the study of mediality in the sense that it articulates the material composition of things and the meaning-making processes associated with them. Following Larkin's insights, we can understand how modes of concealment operate on several levels: they simultaneously provide technical efficiency in the course of action (becoming undetectable), but they also produce symbolic meanings (embodying the fantasy and desire of invisibility) and political subjectivities (ways of acting and organizing, knowing what can be concealed or not). From historical examples to current emergent medialities, we explore how the development of medial forms of concealment intersects with art practices, aesthetics, cultural imaginaries, and political subjectivities in three domains of application: the concealment of physical bodies and objects (camouflage), the concealment of information transmission into a cover medium (steganography), and the concealment of the meaning of information (encryption).

¶15 These three domains related to surveillance and insurgency are emblematic of struggles for power and agency in regimes of visibility. They also allow us to grasp the mediality of digital infrastructures, and they represent rich material with which to analyze the symbolic and imaginary dimensions of sociotechnical practices. This essay aims to contribute to the current studies of mediated in/visibility: first by thinking beyond the dichotomy between visibility and invisibility, and second by taking into account the aesthetic and imaginary dimensions of invisibility. We argue that the way

[8] Brian Larkin, "The Politics and Poetics of Infrastructure," *Annual Review of Anthropology*, vol. 42, 2013, p. 327–343, https://www.annualreviews.org/doi/full/10.1146/annurev-anthro-092412-155522 (accessed 23 October 2018).

tactics of concealment operate on the symbolic level is often detached from their actual technical efficiency.

Camouflage: Towards invisibility cloaks, cyborg spy bugs, and broken dreams

Fig. 2. Women's Camouflage Reserve Corps, of the National League for Women's Service, study camouflage at Van Cortlandt Park, New York, 2018. Photographer: Paul Thompson. NARA.

¶16 In 2017, a video hoax pretending that China had invented a "Quantum Invisibility Cloak"[9] went viral on the Web. Taking root in the old folk tale of the invisibility cloak, the hoax combined elements of truth (the progress of quantum computing) and fiction (the application of this technology in a fully functioning cape). It also operated on the symbolic level to represent the desire of a nation and the fear of its adversaries: China's magical invisibility cloak stands for its rise in power as a technological giant. This example, as well as Ito Steyerl's use of burqas as invisibility cloaks in her video, shows how the old trope of the invisibility cloak is periodically

9 The video is available on YouTube at: https://www.youtube.com/watch?v=ASWJJQkMinc (accessed 23 October 2018).

reactualized to encapsulate power relationships: at the geopolitical level, mastering invisibility is a critical military and intelligence asset. If invisibility cloaks do not exist—at least in the form of fairy-tale capes—the history of military camouflage can be understood as a quest for invisibility, or rather for tactical visibility. It testifies to the relationship of mutual adaptation between modes of concealment and modes of detection in a context of accelerating technological development. A lesser known piece of this history is the role of artists and fiction in the development (and criticism) of military camouflage projects, from the use of paint in World War I to contemporary metamaterials that manipulate electromagnetic waves and biomediality experiments using live organisms as mediums.

¶17 During World War I, France and Great Britain created the first camouflage units in their armed forces, recruiting painters, sculptors, cartoonists, mold-makers, and architects to develop innovative decoy, dummy, and deception techniques. The United States followed quickly and as most of the men had left for combat, the Women's Reserve Camouflage Corps took on the task of creating and testing camouflage strategies to blend into the surrounding environment (see Fig. 2).[10] Meanwhile in London, artists from the Royal Academy contributed to develop the iconic technique of dazzle camouflage. It consisted of painting the fleet of English ships in elaborated zebra patterns. Taking advantage of the progress of zoological science[11] and the formal innovations of modern art, the aim of this dazzle painting was not to make the ships invisible, but rather to hinder the functioning of optical instruments (rangefinders and periscopes) that calculated the trajectory of a ship. The technical efficiency of dazzle painting consisted of breaking up the ship's outline so that detection devices could not focus (see Fig 3). Without the means to calculate the direction and speed of vessels, ballistic attacks could miss their target (although the effectiveness of this technique is debated), leaving time for opponents to reposition and defend themselves. Later, with the invention of new means of detection (radars and the development of aviation), dazzle camouflage became obsolete.

[10] Richard Green, "Hidden Women: The Art of WWI Camouflage," *The Unwritten Record*, 19 June 2016, https://unwritten-record.blogs.archives.gov/2016/07/19/hidden-women-the-art-of-wwi-camouflage-photos/ (accessed 28 July 2018).

[11] The book *Concealing-Coloration in the Animal Kingdom* by Gerald H. Thayer and Abbott Handerson Thayer (London, Macmillan, 1909), is considered a landmark in the field (although its thesis is contested today), followed by zoologist Hugh Cott's book *Adaptive Coloration in Animals* (Oxford, Oxford University Press, 1940). For a contemporary state of the art, see Peter Forbes, *Dazzled and Deceived: Mimicry and Camouflage*, New Haven, CT, Yale University Press, 2009.

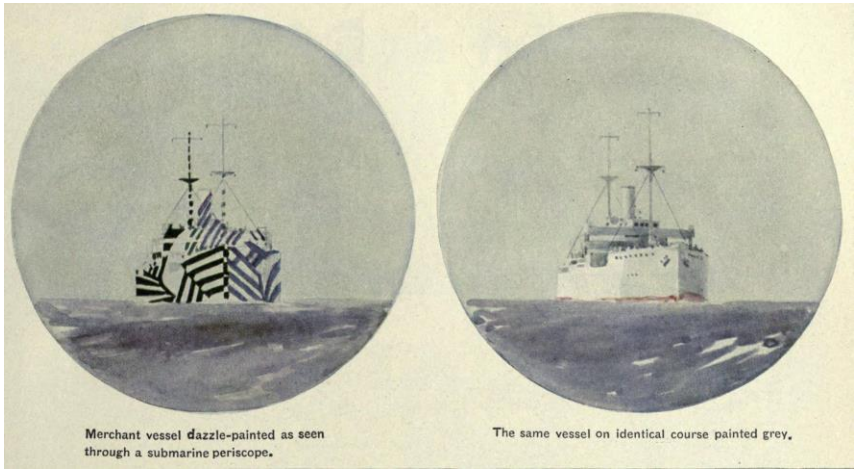

Fig. 3: Example of dazzle painting of ships during World War I. Excerpt from *Encyclopædia Britannica*, 1922. Unknown artist. Public domain.

¶18 New strategies for camouflage on the ground were then developed to deceive pilots' views from the air, such as the creation of false urban networks and fake countryside. Once again, artists and cinema crews were put to work. After the Pearl Harbor attack during World War II, Hollywood set designers were mobilized along with architects and military engineers to hide entire plants and airports under fake landscapes on the American West Coast. Boeing Plant 2 in Seattle was hidden under a 23-acres surface made of plywood and chicken wire imitating an urban neighbourhood suspended 10 meters above the ground. Of unprecedented scale, the decoy landscape featured streets (one jokingly named Synthetic Street), homes, sidewalks, grass, and trees. Figure 4 shows an employee of the Douglas Aircraft Company plant in Santa Monica walking under high veils of burlap mimicking grass patches. But these concealment strategies were themselves thwarted by the improvement of instruments for navigation and aerial detection. And, with the advent of the atomic age, concealment moved more and more underground. Collective paranoia became rich material for many science fiction films that worked to tame the inescapable threat of quasi-supernatural weapons.[12] Interestingly, the journalist and national security expert Glenn Greenwald used the same title as David Bradley's atomic age opus, *No Place to Hide*, in his 2014 book about today's

[12] Cynthia Hendershot and Cyndy Hendershot, *Paranoia, the Bomb, and 1950s Science Fiction Films*, Bowling Green, OH, Bowling Green State University Popular Press, 1999.

technological surveillance.[13] Digital surveillance seems to have replaced the atomic bomb as the utmost invisible and ubiquitous threat in the collective imagination.

Fig. 4: Douglas employee walks underneath the camouflage designed by landscape architect Edward Huntsman-Trout to conceal the manufacture of military aircraft at the Douglas Aircraft Company Santa Monica plant during World War II. 1941–1945. Unknown photographer. Courtesy of the Santa Monica Public Library Image Archives.

¶19 In response to the development of infrared, radar, sonar, and other electromagnetic detection systems, camouflage has had to move beyond the visible spectrum towards stealth shields. Multi-spectral camouflage solutions aim at concealing the signatures of military equipment by assembling various camouflage techniques, from visual camouflage to the concealment of thermal and electromagnetic spectrum signatures. Berlin-based fashion artist Adam Harvey addressed this issue in a project called *Stealth Wear* (2012).[14] He adopted the position of the observed by making camouflage garments intended to disrupt drones' thermic cameras; this, once again, mixed the imagery of cloaks and burqas to address the geopolitical implications of invisibility in counter-insurgency warfare. The closest

[13] Glenn Greenwald, *No Place to Hide: Edward Snowden, the NSA, and the US Surveillance State*, New York, Metropolitan Books/Henry Holt, 2014.

[14] See the artist's website at: https://ahprojects.com/projects/stealth-wear/ (accessed 23 October 2018).

step towards the dream of invisibility cloaking recently reported in the media pertains to the field of "spectral cloaking."[15] This technique manipulates the frequency of light waves as they pass through an object, rendering it invisible to the observer monitoring the wave, and potentially undetectable on the entire electromagnetic spectrum. Yet recent studies [16] conclude that there is a mathematical limit on broadband cloakability, given that rendering an object invisible in the optical field requires the use of electromagnetic materials that can make the cloaked object even more detectable on an electromagnetic field.

¶20 Rather than making objects disappear, current developments in camouflage explore the use of animal shapes and bodies to render surveillance devices undetectable. Intelligence gathering robots and cyborgs can be considered contemporary versions of the Trojan horse. Just as the shapes and behaviours of animals inspired the first military camouflage techniques, many prototypes of miniaturized Unmanned Aircraft System (UAS, or Micro Air Vehicle, MAV) mimic the look and behaviour of animals to blend high-tech devices into natural and urban environments. Examples include prototypes of DARPA's AeroVironment Nano Hummingbird equipped with a camera that can enter buildings and perch on power lines to recharge batteries. While biomimesis (the imitation of other living organisms' biological systems and ethology)[17] has long been a source of inspiration for human concealment techniques, bionic engineering innovations in the twentieth and twenty-first centuries have pushed the limits of the medial forms of concealment. In 2006, DARPA published a contractor solicitation to develop Hybrid Insect Micro-Electro-Mechanical Systems (HI-MEMS),[18] dubbed "cybug program." Its aim is to implant bio-electromechanical interfaces into insects (moths, beetles, dragonflies, and other swimming and hopping insects) to harvest power from their body, control their locomotion systems and use them for advanced reconnaissance missions in

[15] Luis Romero Cortés, Mohamed Seghilani, Reza Maram and José Azaña, "Full-Field Broadband Invisibility through Reversible Wave Frequency-Spectrum Control," *Optica*, vol. 5, no. 7, July 2018, https://doi.org/10.1364/OPTICA.5.000779 (accessed 23 October 2018).

[16] Francesco Monticone and Andrea Alù, "Invisibility Exposed: Physical Bounds on Passive Cloaking," *Optica*, vol. 3, no. 7, 2016, p. 718–724.

[17] On this topic see Roger Stahl, "Life Is War: The Rhetoric of Biomimesis and the Future Military," *Democratic Communiqué*, vol. 26, no. 2, Fall 2014, p. 122–137.

[18] DARPA, "Hybrid Insect MEMS (HI-MEMS). Solicitation Number: BAA06-22," *Federal Business Opportunity*, 2006, https://www.fbo.gov/index?s=opportunity&mode=form&id=ec6d6847537a922081of4282eeddaod2&tab=core&_cview=1 (accessed 27 July 2018).

enemy territory. The ultimate plan, according to technology editor Colin Johnson, is to "eventually hack into the insects' own natural senses, allowing the remote-control operator to look out of the insects' own eyes, instead of attaching a video camera for it to carry."[19]

¶21 For the launch of the HI-MEMS program, science fiction author Thomas Easton received an invitation (which he declined) from DARPA's program director Amit Lal. The latter said he enjoyed Easton's 1990 novel *Sparrowhawk* in which the author imagines animals enlarged through bioengineering, equipped with implanted control systems. The invitation stood as a joint celebration of the book's visionary technological imagination (or dystopia) and of the scientific achievement of DARPA's in moving closer to the creation of cybugs. While we are still far from deploying swarms of autonomous cybugs, biorobotics is advancing quickly in this field, now allowing us to control the flight of a beetle with a Wii remote control.[20] DARPA's history, however, is "littered with broken dreams."[21] But these dreams are well-alive in fiction works. In a feedback loop from scientific development to science fiction, the 2015 British thriller film *Eye in the Sky*, directed by Gavin Hood, captures very well the use of biologically inspired micro drones—a hummingbird and a beetle—in the context of counterterrorism. Opposing UK intelligence to Middle Eastern insurgents, the plot addresses the ethics of drone warfare. Contrary to the old myth of the invisibility cloak, which evokes magic and fairy-tale imaginaries (as, for example, in its recent revival in the Harry Potter novels and movies), insurgency scholar Paul Rich notes that the cinematic representation of Unmanned Aircraft System tends to be associated with negative imagery and creates false impressions of imperial omnipotence.[22]

¶22 This brief history of camouflage traces an evolution of medial forms of concealment in which aesthetics and art practices are woven into military and intelligence practices. They operate both at the level of technical efficiency (the crafts of producing visual effects to trick the enemy) and at the level of symbolic power (the

[19] Colin R. Johnson, "Darpa Hatches Plan for Insect Cyborgs to Fly Reconnaissance," *Electrical Design News*, 3 October 2007, https://www.eetimes.com/document.asp?doc_id=1167200 (accessed 27 July 2018).

[20] Evan Ackerman, "Controllable Cyborg Beetles for Swarming Search and Rescue," *IEEE Spectrum*, no. 28, November 2017, https://spectrum.ieee.org/automaton/robotics/robotics-hardware/cyborg-beetles-for-swarming-search-and-rescue (accessed 27 July 2018).

[21] Johnson, 2007.

[22] Paul B. Rich, "Cinema, Drone Warfare and the Framing of Counter-Terrorism," *Defense & Security Analysis*, vol. 34, no. 2, 2018, p. 1–17.

mobilization of mythological and science fiction references to convey the image of supernatural technological achievements detached from actual efficiency). The next section moves away from the concealment of bodies and equipment (camouflage) to analyze the medial forms of information-hiding and their evolution in the context of digital media and biotechnologies, leading further into the "deep mediatization"[23] of the world.

Steganography: Information-hiding and life forms as cover media

¶23 The relationship between visible surface and concealment is key to the *modus operandi* of steganography, or "covered writing." Steganography is the craft of hiding an underlying secret message within a cover medium, for example a physical surface that displays a mundane texture, a random pattern, or an ordinary message escaping scrutiny. The Ancient Greek historian Herodotus testified to one of the earliest known steganographic techniques. In book V of his *Histories*,[24] he recounts how Histiaeus had a message tattooed on the skull of his most trusted servant, then waited until the hair grew again and sent the messenger across the enemy's roadblocks, bringing instruction to revolt. The development of steganographic techniques has expanded into an increasingly diverse array of media of information storage and transmission. As breakthrough experiments seem to be turning any material form into a potential cover medium that can store and transmit sensitive information, efforts to legitimize or delegitimize these new techniques of concealment operate both on aesthetic and moral grounds.

¶24 Contemporary steganographic techniques can conceal information in digital signals, streams, and data files, especially in large media files such as images, audio clips, and videos. "Noise" in the data is modified to encode hidden messages, often encrypted to add extra security. For example, JPEG images can be used as carriers to hide another medium (an image, a text file, or an audio file) within the code of the cover image file: one way to achieve this is to identify redundant bits in the image bitmap, select a subset of such bits and replace them with data from a secret message.[25] In this case, the visual surface stands as a deceiving screen, hiding sensitive information in the background code. Some of the most elaborate techniques of

[23] Nick Couldry and Andreas Hepp, *The Mediated Construction of Reality*, Cambridge, MA, Polity Press, 2017.

[24] Herodotus, *The History of Herodotus*, c. 440 B.C., trans. by Georges Rawlinson, http://classics.mit.edu/Herodotus/history.5.v.html (accessed 23 October 2018).

[25] Hanna Rose Shell, *Hide and Seek: Camouflage, Photography, and the Media of Reconnaissance*, Cambridge, MA, MIT Press, 2012.

digital steganography pertain to the category of network steganography. They consist of hiding information in user-to-user traffic or in machine-to-machine signal transmission. For example, secret messages can be introduced in delayed or corrupted data packets sent during Voice-over-IP conversations, or they can be concealed within the inter-protocol features of networks. In the case of blog-steganography, the blogosphere itself becomes the carrier of hidden messages: the piece of information used to conceal is fractionalized and its parts are distributed to a selection of websites and posted in the comments sections of abandoned blogs. More generally, all platforms that allow users to post user-generated content can be used to hide steganographic data in the open.

¶25 In 2005, Gordon Thomas claimed in his book *Gideon's Spies: The Secret History of the Mossad*[26] that Isis and al-Qaeda members communicated secret messages through eBay and Reddit. Encrypted information was purportedly hidden in photographs of goods offered for sale online as well as in pornographic images posted on discussion threads. Even before the terrorist attacks of September 11, the use of pornographic images for steganography by Islamic counter-insurgents was widely relayed in Western media, thus contributing to a discourse that discredited insurgents on moral grounds.[27] These news stories triggered a debate among tech experts and media scholars, some claiming that the likelihood of terrorist groups disseminating steganographic material on the Web was small,[28] while others hypothesized that such news reports were mere vehicles for an "elaborate government disinformation campaign aimed at vilifying encryption, in particular, and the Internet, in general, in order to gain public consent for its control."[29] Since the peak of this debate in 2001–2002, various media reported new cases of terrorist investigations leading to the discovery of steganographic material hidden in porn

[26] Gordon Thomas, *Gideon's Spies: The Secret History of the Mossad*, [1999], New York, St. Martin's Griffin, 2005.

[27] Jack Kelley, "Terror Group Hide behind Web Encryption," *USA Today*, 2 May 2001.

[28] Robert J. Bagnall, "Reversing the Steganography Myth in Terrorist Operations: The Asymmetrical Threat of Simple Intelligence Dissemination Techniques Using Common Tools," *SANS Institute*, 2002, https://www.sans.org/reading-room/whitepapers/stenganography/reversing-steganography-myth-terrorist-operations-asymmetrical-threat-simple-intellig-556 (accessed 30 July 2018).

[29] Sandor Vegh, "Hacktivists or Cyberterrorists? The Changing Media Discourse on Hacking," *First Monday*, vol. 7, no. 10, 2002, http://firstmonday.org/article/view/998/919 (accessed 30 July 2018).

files.[30] Some of these news reports tend to bolster the fear that "steganography could turn the internet into the ultimate 'dead drop'," as stated in a 2005 ABC TV program.[31] Such triggers of moral panic around emerging technologies are somehow reminiscent of more recent fake rumors that the Bitcoin blockchain could contain secret child pornography. For blockchain expert Kai Sedgwick, while it is "possible to encode a hidden link inside any database [...] [t]he act of doing so proves nothing other than the fascination some people have for concealing messages in messages"[32]—as well as tendencies to answer tech anxiety with disproportionate moral outrage against sexual imagery, perversion, and secrecy.

¶26 While digital steganography and the blockchain have been associated with negative representations of concealment, the early development of DNA steganography is (so far) characterized by narratives of virtuosity, anchored in references to artistic mastery. Research in biochemical data storage at the molecular level is quickly moving forward with methods of successfully encoding information into DNA base sequences—the chemical units of code A, T, G, and C. Bioinformatics advances may be on the verge of making DNA just another type of storage medium (yet still costly)[33] to archive books, images, videos, and complete computer operating systems—and to hide and protect secret information. Microsoft plans to get a prototype DNA storage system fully operational inside one of its data centres by 2020, envisioning that it will fit the content of entire data centres into the palm of the hand.[34] As a data storage medium, DNA extends the range of medial forms that can be used to conceal sensitive information.[35]

---

[30] Nic Robertson, Paul Cruickshank and Tim Lister, "Documents Reveal al Qaeda's Plans for Seizing Cruise Ships, Carnage in Europe," *CNN*, 1 May 2012, https://edition.cnn.com/2012/04/30/world/al-qaeda-documents-future/index.html (accessed 30 July 2018).

[31] Catalyst, *ABC.net*, 10 March 2005, http://www.abc.net.au/catalyst/stories/s1320215.htm (accessed 30 July 2018).

[32] Kai Sedgwick, "No, There Isn't Child Porn on the Bitcoin Blockchain," Bitcoin.com, 21 March 2018, https://news.bitcoin.com/no-isnt-child-porn-bitcoin-blockchain/ (accessed 29 October 2018).

[33] Darshan Panda, Kutubuddin Ali Molla, Mirza Jainul Baig, Alaka Deeptirekha Swain, Behera and Manaswini Dash, "DNA as a Digital Information Storage Device: Hope or Hype?," *Biotech*, vol. 8, no. 5, 2018, p. 3.

[34] See the company Catalog's vision for providing platform scale, long-term archival of data: https://catalogdna.com/about/ (accessed 28 July 2018).

[35] Ho Bae, Byunghan Lee, Sunyoung Kwon and Sungroh Yoon, "DNA Steganalysis Using Deep Recurrent Neural Networks," *ArXiv Preprint*, https://arxiv.org/abs/1704.08443 (accessed 28 July 2018).

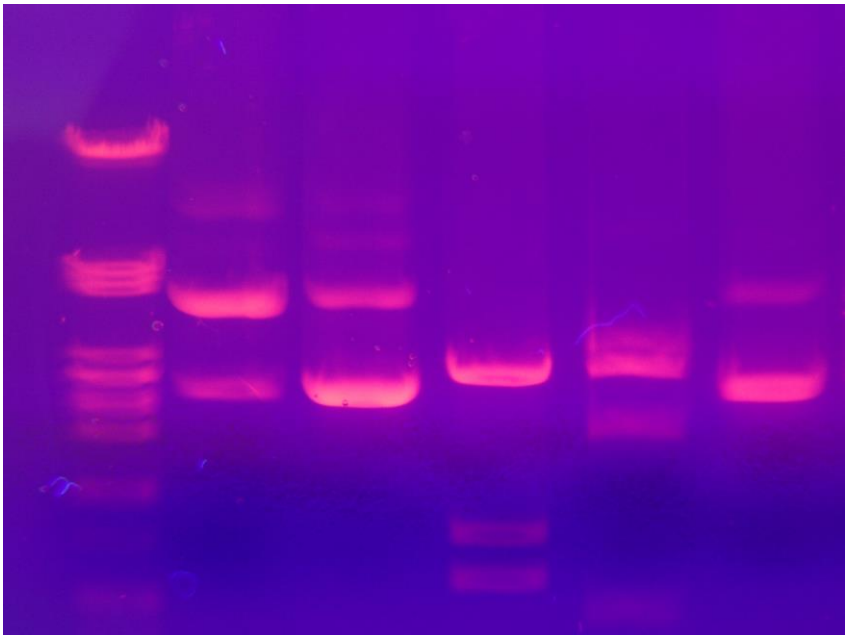

Fig. 5: Electrophoresis gel revealing six DNA tracks. Photography: Mnolf. GFDL & CC ShareAlike 2.0, Wikimedia Commons.

¶27 Some of the first groundbreaking innovations in the field of DNA information storage were achieved through the collaboration of artists and molecular biologists working on the DNA of *E. coli* bacteria. In 1988, artist Joe Davis partnered with scientists at MIT to create the artwork *Microvenus*: an ancient Germanic rune representing fertility encoded into a bacteria DNA.[36] Various groundbreaking experiments in biomolecular computation also implied the remediation of artworks and historical cultural artefacts. In 2015, the Davos Bitcoin Challenge asked researchers to retrieve a Bitcoin private key encoded in the content of DNA-tubes, allowing the winner to claim one bitcoin as a reward. Along with the Bitcoin key the winner also retrieved a drawn portrait of novelist James Joyce encoded in the content of the DNA-tube. To explain the meaning of this reference to Joyce, we offer the hypothesis that the portrait hints to Joyce's aesthetic conception of the visible and the surface. The following excerpt from his masterpiece *Ulysses*,[37] where the character

[36] Joe Davis, "Microvenus," *Art Journal*, vol. 55, no. 1, 1996, p. 70–74.

[37] Cited in Ernesto Livorni, "Ineluctable Modality of the Visible: Diaphane in the 'Proteus' Episode," *James Joyce Quarterly*, vol. 36, no. 2, 1999, p. 127–169.

Stephen Dedalus ponders on his stream of consciousness, denotes striking cues to the process of decoding DNA in the context of the Bitcoin challenge:

> Ineluctable modality of the visible: at least that if no more, thought through my eyes. Signatures of all things I am here to read, seaspawn and seawrack, the nearing tide, that rusty boot. Snotgreen, bluesilver, rust: coloured signs. Limits of the diaphane. But he adds: in bodies. Then he was aware of them bodies before of them coloured. How? By knocking his sconce against them, sure. Go easy. Bald he was and a millionaire, maestro di color che sanno. Limit of the diaphane in. Why in? Diaphane, adiaphane. If you can put your five fingers through it, it is a gate, if not a door. Shut your eyes and see.

Evoking visibility beyond the limits of perception, this fragment resonates with the aesthetics evoked by the Bitcoin challenge: a bald millionaire-to-be searching for hidden signatures within bodily material by mastering colours (in DNA extraction, molecules are tagged with fluorescent dyes). Besides the Bitcoin challenge, a strikingly high number of DNA-encoding breakthroughs intentionally associate themselves with a repertoire of art pieces. In a previous 2013 exploit, molecular biologist Nick Goldman, founder of the Bitcoin challenge, encoded 739 kilobytes of data into DNA including all 154 of Shakespeare's sonnets. Three years later, Microsoft stored 200 megabytes into DNA material, among which the top 100 books from Project Gutenberg and the video "This Too Shall Pass" by the band OK Go. In the video, members of the band are accompanied by musicians wearing ghillie suits, a type of camouflage clothing blending the characters into the grass and foliage.[38]

¶28 As the above examples show, scientists and biotechnology companies are actively working on building an aesthetic dimension into the practice of DNA encoding. Contrary to the negative representation of steganography that came to be associated with a moral condemnation of criminal activities, pornography, and pedophilia, the aesthetics of concealment in DNA is carefully crafted by scientists and IT companies. The emergent medial form of DNA encoding is actively correlated with the classical themes of the surface—invisibility and camouflage—through the mobilization of a legitimate cultural repertoire that traces a continuity between past and present and situates the performance of scientists in the lineage of prestigious figures: symbols of art mastery (Shakespeare, Joyce), icons of media history

[38] The video is accessible at: https://www.youtube.com/watch?v=UJKythlXAIY (accessed 23 October 2018).

(Muybridge[39]) and pop celebrities (OK Go). The structures of feeling produced by these aesthetics stimulate the senses of pride and desire—and contribute to relegate ethical concerns to the background.

Encryption: Concealing content, know-how, and infrastructure

¶29 Steganography is usually employed in combination with encryption to strengthen its efficiency. Etymologically, the Ancient Greek word *kruptós* means hidden, concealed, private, and secret. As a technique, encryption conceals information by means of a code. It can be described as a process of encoding messages, which are only "visible" or "readable" to those who have the appropriate key, code, or cypher, to decipher them. This technique has been used for centuries. In the *Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*,[40] David Kahn documents the history of cryptography from Ancient Egypt up to 1967, when the book was first published. He examines many of the various cyphers developed over time to conceal content. Handwritten cyphers serve as a basis for today's automated and digital encryption. More recently, the development and use of encryption technologies has exploded and been seen by many, particularly techies, as a solution to mass surveillance, following Edward Snowden's revelations.

¶30 A number of interrelated dynamics are at play when it comes to digital encryption. These include cypher/non-cypher, encryption/decryption, symmetry/asymmetry, and visibility/invisibility. The type of content that can be encrypted with contemporary techniques ranges from an email message, a discussion list, a WhatsApp conversation, a computer hard disk, a file, a folder, or a pen drive, among many others. When using digital encryption to send and receive messages, only a fraction of the data transmitted is in fact concealed. While the main message is encrypted, most of the metadata—often the most valuable information, such as the time the message was sent or the person to whom it was addressed—is not encrypted. To decrypt an encrypted message, the receiver needs a code, otherwise the message remains a form of gibberish—a long string of numbers and letters—to those who do

[39] Seth L. Shipman, Jeff Nivala, Jeffrey D. Macklis and George M. Church, "CRISPR–Cas Encoding of a Digital Movie into the Genomes of a Population of Living Bacteria," *Nature*, vol. 547, 2017, p. 345–349, https://dash.harvard.edu/bitstream/handle/1/35982200/5842791.pdf?sequence=1 (accessed 23 October 2018).

[40] David Kahn, *The Codebreakers: The Comprehensive History of Secret Communication from Ancient Times to the Internet*, [1967], New York, Scribner, 1996.

not have the proper key to decrypt it. Encryption can be symmetric or asymmetric, meaning that the keys (or codes) needed to decrypt a message are either similar for the sender and receiver, or dissimilar (i.e. asymmetric).

¶31 To function properly, digital encryption relies on know-how (such as the expertise needed to install the appropriate software and the skills necessary to not be intercepted), telecommunication infrastructure (such as the undersea cables, fiber optic, computers, and servers) and networks of contacts (such as friends and colleagues who can use encryption)—and at times unsuspected medial forms such as pen and paper. These three aspects encapsulate well the necessary, but often "forgotten," infrastructure needed for developing and using encryption (i.e. people, material, and techniques). Moreover, when focusing on encryption, the affective and ritual dimensions involved are far from sight. Additionally, the emblematic case studies of the development and use of encryption in the literature (such as the Diffie-Hellman [DH] and Rivest-Shamir-Adelman [RSA] encryption algorithms), and encryption tools (such as PGP and TOR), or cryptanalysis techniques (such as the decryption of Enigma by Alan Turing and his team) are those located in the Global North rather than those in situations of oppression in the Global South and/or by and about subjugated people. Focusing on the latter examples reveal stories of what has largely remained under the radar in the history of encryption.

¶32 Digital encryption is employed for many purposes. One of its applications is to secure data that allows capital to flow. Whether it is used for small transactions, such as paying one's online bills or buying a product on the Internet, or for high capital flows, encryption conceals sensitive information (such as credit card numbers) with the hope that it will not be intercepted. At the level of tactical organization (such as using encryption by hackers and/or activists to organize), the use of digital encryption conceals the prior proficiency and know-how necessary to use such technique. To use encryption one needs to have the appropriate computer skills to install and properly manage encryption program(s) such as PGP. The use of encryption for tactical organizing also requires the user to know how to manage digital signatures (signatures that some hackers only give when meeting face-to-face). This means that one often needs to be part of a web of trust (a network of contacts) to connect with people through encryption.

¶33 Until recently, encryption was a technique that only a few experts used, and it is now being adopted by many ordinary users on an everyday basis through digital tools like Signal, Telegram, or WhatsApp. These tools no longer require the users to have the advanced skills needed to understand the process of encryption. The know-how and the network of contacts with such technical knowledge is no longer a barrier

to access. The mainstreaming of such tools has facilitated the use of encryption to provide privacy and security to everyday data communication. Moreover, this mainstreaming has facilitated access to encryption because of the widespread use of devices (often through smart phones) in addition to growing Internet infrastructures: many undersea cables have been built in the Global South in the last 10 years and terrestrial fiber optic networks have been installed in urban areas.

¶34 The ritual and affective dimensions of encryption are often overlooked in frameworks that emphasize its technical aspects. Among hackers, the signing of digital keys to communicate by email with PGP—an activity that confirms you are a trusted person within an encryption web of trust—has become a ritualized event. During hacker meetings, it is not rare to have "key signing parties" where all who want to attend will sign their public key face-to-face. Assembled in circles or in lines, participants (often white men) one by one recite out loud their public key—a long string of numbers—and thereby confirm that they are the ones behind their public key. In some cases, ID documents provide visual proof of identity. At this point, no digital media is involved: speech, pen, and paper are the sole accepted means of information transmission. It is through this process that members of an encryption network become fully trusted interlocutors since the authentication of their key was done face-to-face. This exercise can take a few hours depending on the number of participants. Once members have gone through this ritual, they become part of the web of the fully trusted.

Fig. 6: Key signing party as FOSDEM 2008, Stevenfruitsmaak, Wikimedia Commons CC BY 2.5.

¶35 The case of key signing parties illustrates how encryption now and then engages an infrastructure of people, techniques, and material forms, including assemblages of mediated and non-mediated means of communication. If the history of encryption can in part be read through the lens of technological acceleration—leading to the current race for quantum-resistant encryption techniques—it also testifies to the craft of assembling old and new forms of communication to create opacity.

¶36 For example, during World War II, code talkers were used to communicate secretly and transnationally by the American and Canadian armies, among others. The peculiarity of this form of encryption was that it relied on orality (like key signing parties). Code talkers were Indigenous people who would communicate between Europe and North America using their indigenous mother tongue.[41] This was considered to be an oral way to encrypt communication since so few people could understand languages such as Navajo (USA) and Cree (Canada). The use of military telephone or radio communication nets to mediate the sharing of strategic information was seen as a secure and fast way to encrypt communication across borders. While during the war the knowledge of Indigenous languages was understood as a strategic advantage by the Canadian government, in the post-war context, and before, Indigenous children were often prohibited from speaking their mother tongue. This was based on a policy where Indigenous people would "cease to exist as distinct legal, social, cultural, religious, and racial entities in Canada."[42] This colonial policy has led to the current state of affairs where Indigenous languages are either vulnerable, endangered, or extinct.

¶37 In the context of liberation or independence movements in the Global South, the use of non-automated encryption was mobilized as a way to conceal strategic information exchange over space. Che Guevara and Fidel Castro exchanged coded messages to communicate secretly using a One-Time Pad (OTP) booklet.[43] With proper OTP booklets, they could understand each other's messages, whereas others who have put their hands on the coded message, but not on the booklet to decipher

[41] Alexandra Lazarowich and Cowboy Smithx, *Cree Code Talker*, 2015, https://www.youtube.com/watch?v=7JiUPBKST5M (accessed 2 July 2018).

[42] Truth and Reconciliation Commission of Canada, *What We Have Learned: Principles of Truth and Reconciliation*, Government of Canada, 2015, http://nctr.ca/assets/reports/Final%20Reports/Principles_English_Web.pdf (accessed 2 July 2018).

[43] Craig P. Bauer, *Secret History: The Story of Cryptology*, Boca Raton, FL, CRC Press, 2013, p. 575.

it, would only see gibberish. The access to the nature of the message was thus protected by the encryption/decryption key, which at the time was symmetric (i.e. both parties needed the same key—the OTP booklet—to decipher each other's messages).

¶38 Over the years, techniques of encryption and their affiliated infrastructure have evolved and become more sophisticated. From the use of hand-written cryptography to communicating via radio with secret languages, encryption has slowly become automated, increasing, among other things, the speed of encrypted long-distance communication. A notable example is the development and use of an automated encrypted communication system that took place in the 1980s during the anti-apartheid struggle, which enabled freedom fighters to communicate secretly and transnationally.[44] Since the 1960, the African National Congress had been banned in South Africa and most of its senior leadership was in exile in Lusaka, Zambia. The encrypted communication system based on an automated One-Time Pad channeled all communication from South Africa to Zambia via London, UK. When a freedom fighter wanted to send a message from Johannesburg, she first needed to encipher it with a diskette on which the encryption program was saved. Then it was passed through a computer's serial port to an acoustic coupler modem. The computers and diskettes had been imported earlier by a mule who doubled as a flight attendant. The digital data was then converted to sound, and was recorded on a small cassette tape recorder. The freedom fighter would then call London, play the encrypted audio message, and the text would automatically be recorded on an answering machine. To decrypt the message, the same process would be used but in reverse. Using an encrypted telematics system (phone + computer) increased the speed at which messages could be exchanged across borders. It also countered surveillance from the South African white supremacist regime with the aim of supporting the efforts to overthrow that regime, which had been in place since 1948. Its infrastructure was completely invisible to the regime and, because of its secret nature, was only known to a handful of freedom fighter cadres. In this case, the web of trust was small as most anti-apartheid activists had no idea that the system existed. It is only when the system

[44] Kelly R. Garrett and Paul Edwards, "Revolutionary Secrets: Technology's Role in the South African Anti-Apartheid Movement," *Social Science Computer Review,* vol. 25, no. 1, 2007, p. 13–26. Sophie Toupin, "Gesturing Towards 'Anti-Colonial Hacking' and Its Infrastructure," *The Journal of Peer Production*, no. 9, 2016, http://peerproduction.net/issues/issue-9-alternative-internets/peer-reviewed-papers/anti-colonial-hacking/ (accessed 29 July 2018).

was exposed by accident that the encrypted communication infrastructure was revealed in 1990, two years after it began to function.

¶39 Encryption requires an assemblage of people with skills, the availability of a telecommunication infrastructure, and a variety of interconnected techniques that can combine low- and high-tech. The use of encryption often conceals those components and makes them appear as purely technical. Rendering them visible brings to the fore the hidden infrastructure necessary to make encryption function seamlessly.

Conclusion

¶40 This introduction proposed a cultural analysis of three emblematic concealment procedures through the lens of their intermedial logics. Exploring the coevolution of materiality and symbolic meanings in the fields of camouflage, steganography, and encryption, we unraveled some of their profound entanglements in technological, aesthetic, and political logics. In these three fields, the material assemblages allowing for concealment tend to become more and more technologically complex, from cinema crafts to metamaterials and biomediality. They sometimes rely on whole infrastructures, including networks of contacts and webs of trust. Yet to deceive expectations or gain efficiency, they can also include non-mediated forms of communication and old media (pen and paper, face-to-face identification of interlocutors, oral transmission in aboriginal language, human mules) creating multiple intermedial assemblages.

¶41 The arts and techniques of concealment not only operate on the level of practical efficiency, but also on the level of symbolic meanings. They carry (and are shaped by) representations and social imaginaries that can impact our relationship to the world as well as the constitution of subjectivities. Technologies of concealment embody the fantasies, hopes, and dreams of an epoch, from the fascination with electromagnetic invisibility cloaks to the awe generated by DNA encoding to the paranoid fear of ubiquitous data capture and militarized cyborg insects. Operating on the aesthetic level by reorganizing the perceptual and sensible field, they contribute to creating a sense of uncertainty and suspicion towards our environments. What kind of subjectivity may adapt to a world in which every single physical phenomenon seems potentially exploitable as a medium of concealment? Peter Eckersley, former staff technologist at the Electronic Frontier Foundation, argues that "[i]f people in a free society have to start worrying that any insect they see might be conducting surveillance, then that could seriously inhibit their ability to

develop their character and express themselves."[45] Indeed, these almost surreal performances of concealment "enter into our unconscious and hold sway over the imagination."[46] Projecting symbolic power (especially state power, in the case of intelligence and warfare), they simultaneously create awe and desire, intimidation, and resource attraction—even if they are practically ineffective as means of concealment. As a matter of fact, the effectiveness of dazzle painting has always been contested, broadband cloakability faces some serious limitations, and camouflaged UAV tend to bolster false impressions of imperial omnipotence. Broken dreams "can take on fetish-like aspects that sometimes can be wholly autonomous"[47] from their failed technical performance, especially when their inventors deploy active strategies of legitimation by associating their experiments with a wide range of famed cultural symbols, from mythology and classical literature to science fiction and pop culture.

¶42 The financial and infrastructural resources necessary to produce ultra-sophisticated techniques of concealment can also be read as "embodiments of objective historical forces."[48] Most of the devices built to keep up with the accelerating pace of detection and concealment dynamics are only affordable to state agencies and well-funded scientists and industries. Yet light tactical organizations are not limited to deceleration strategies, as evinced by examples from anti-colonial struggles. Hacking into powerful devices and infrastructures of concealment can also have a high impact with low financial investment. In Easton's 1990 novel, the insurgents manage to hack into the systems of cyborg insects and turn them against their masters. Yet in the case of the contemporary cyborg moths program under development at DARPA, Easton recommends a more basic low-tech solution: "Imagine a thousand moths released to search for insurgent activity—all the insurgents would have to do is build a bonfire to attract them, then use pesticides or bug-zappers to kill them."[49]

[45] Cited in Johnson, 2007.
[46] Larkin, 2013, p. 333.
[47] *Ibid.*, p. 329.
[48] *Ibid.*, p. 333.
[49] Cited in Johnson, 2007.

The Mediality of Concealment: Material Practices and Symbolic Operativity

Nathalie Casemajor, Institut national de la recherche scientifique
Sophie Toupin, McGill University

RÉSUMÉ

Ce numéro spécial porte sur les formes culturelles, les technologies et les logiques sociales de la dissimulation. Nous proposons dans cette introduction un examen critique des enchevêtrements culturels et politiques de trois domaines emblématiques de la dissimulation : le camouflage, la stéganographie et l'encryption. Centrée sur l'étude de la médialité, notre analyse croise l'évolution des environnements médiatiques et des représentations de ces procédés de dissimulation pour mieux en comprendre les modes de légitimation et l'opérativité symbolique.

ABSTRACT

This special issue focuses on the cultural forms, technologies, and social logics of dissimulation. In this introduction, we propose a critical examination of the cultural and political entanglements of three emblematic domains of dissimulation: camouflage, steganography, and encryption. Focusing on the study of mediality, our analysis crosses the evolution of media environments and representations of these dissimulation processes to better understand their modes of legitimization and symbolic operativity.

NOTES BIOGRAPHIQUES

Nathalie Casemajor is an Assistant Professor in the Urbanisation Culture Société Research Centre at INRS (Institut national de la recherche scientifique) in Montreal. Her work focuses on cultural development and digital culture. She is the coordinator of the Observatory of Cultural Mediations and coedited the book *Expériences critiques de la médiation culturelle* (PUL, 2017). She also conducted research projects on cultural institutions and Wikipedia, arts, and public space and the circulation of news and artworks on the Web.

Sophie Toupin is a PhD candidate in the Department of Art History and Communication Studies at McGill University. Her doctoral research examines the relationship between communication technologies and revolutionary movements. Her secondary research interest explores the linkages between technology, feminism,

and activism. Her work has been published in *Ada: A Journal of Gender, New Media, and Technology*; *Canadian Journal of Communication*; *Journal of Peer Production*; and *Cahiers du gerse*, among others.