eğitim bilim toplum
Üç aylık hakemli dergi

Hakemli Makale

The Dualist Nature of Technologist Resistance: The Case of the Cypherpunks

Ahmed Al-Madhoun*

Geliş Tarihi / Received: 22 Mayıs 2026 **Kabul Tarihi /** Accepted: 24 Haziran 2026

Al-Madhoun, A. (2026). The Dualist Nature of Technologist Resistance: The Case of the Cypherpunks. *Eğitim Bilim Toplum*, 24 (2), 198-217

Abstract

Counter-surveillance is a corollary of surveillance. The perfection of a control regime does not preclude different forms of resistance. One form of resistance emerging with the digital paradigm is Technologist Counter-Surveillance, which emphasises the primacy of creating and developing technological tools against the contemporary surveillance regime. Nevertheless, there is a dilemma at the heart of this approach. While being a disturbing force which caused significant ameliorative outcomes with pivotal emancipatory role, technologist counter-surveillance have also reinforced power relations in the information regime. To understand this dilemma, this paper investigated the Cypherpunks as an exemplary case of Technologist Counter-Surveillance. It analysed them in the context of the information regime as a form of control operating according to the imperatives and dynamic of psychopolitics developed by Byung-Chul Han. The paper demonstrates that Technologist counter-surveillance takes place necessarily within the information regime, which is the same regime it tries to counter. It is of a dual character: at once disruptive of, and reinforcing the information regime.

Key Words: Surveillance, counter-surveillance, technologist resistance, information regime, Cypherpunks.

* **PhD Student, Middle East Technical University, Email: linguaphile.ahmed@gmail.com Orcid Number: 0009-0002-0251-3339**
Doktora Öğrencisi, Orta Doğu Teknik Üniversitesi, E-posta: linguaphile.ahmed@gmail.com Orcid Numarası: 0009-0002-0251-3339

Teknolojist Direnişin Düalist Doğası: Cypherpunklar Örneği

Öz

Gözetime karşı koyma, gözetimin doğal bir uzantısıdır. Bir kontrol rejiminin kusursuzlaşması, farklı direniş biçimlerinin ortaya çıkmasını engellemez. Dijital paradigma ile birlikte beliren direniş biçimlerinden biri, çağdaş gözetim rejimine karşı teknolojik araçlar üretme ve geliştirme önceliğini vurgulayan Teknolojist Gözetime Karşı Koyma'dır. Bununla birlikte, bu yaklaşımın merkezinde bir ikilem yer almaktadır. Teknolojist gözetime karşı koyma, merkezi bir özgürleştirici role sahip sarsıcı bir güç olarak önemli ölçüde iyileştirici sonuçlar doğururken, diğer yandan enformasyon rejimindeki iktidar ilişkilerini de pekiştirmiştir. Bu ikilemi anlamak adına bu çalışma, Teknolojist Gözetime Karşı Koyma'nın örnek bir vakası olarak Cypherpunkları incelemektedir. Çalışma, bu topluluğu, Byung-Chul Han tarafından geliştirilen psikopolitikanın buyrukları ve dinamiklerine göre işleyen bir kontrol biçimi olan enformasyon rejimi bağlamında analiz etmektedir. Makale, Teknolojist gözetime karşı koymanın, karşı çıkmaya çalıştığı rejimin ta kendisi olan enformasyon rejiminin içinde zorunlu olarak varlık gösterdiğini ortaya koymaktadır. Bu bağlamda söz konusu eylem; hem ilerici hem gerici, hem sarsıcı hem de pekiştirici niteliğiyle ikili (düalist) bir karaktere sahiptir. Dahası, bu yapısı gereği, karşı koymaya çalıştığı rejim ve onun buyruklarıyla kurduğu iç içelik ölçüsünde, gözetime karşı koymadaki etkililiği de sınırlı kalmaktadır.

Anahtar Sözcükler: Gözetim, teknolojist direniş, gözetime karşı koyma, enformasyon rejimi, Cypherpunks.

Introduction

Last June, 2025 witnessed the largest data breach in history, containing 16 billion passwords from Big Tech companies, including Facebook, Apple, and Google. However, in the contemporary digital surveillance regime, data breaches happen almost every day. It is an era where surveillance is omnipresent with different guises and for interests, ever increasing the risk of exposure. Despite the historical ubiquity of Surveillance, and the phenomena associated with it (Weller, 2022), novel features and forms emerged along with the digital paradigm. It has become both pervasive and intrusive, occupying new spaces and penetrating new depths.

This notwithstanding, the digital paradigm possessed an emancipatory potential and promise. Indeed, a plethora of examples demonstrate the positive impact of these technologies in terms of disturbing dominant narratives and casting light on different injustices and inequalities (Sewell, 2022; Maxigas, 2015; Skare, 2018; Yu et al., 2022). Moreover, the corollary of a surveillance system are the attempts to destruct or reduce its efficacy and harm. These forms of resistance are complex, varying and dynamic (Baaz et al, 2023; Lilja et al, 2017; Lilja, 2020; Ettlinger, 2018). One form of counter surveillance is '*Technologist Counter-Surveillance*'.

Technologist counter-surveillance refers to the approach emphasising the primacy of digital technology itself as means and strategy of resistance against the information regime. Technology shapes the tactics, modes and forms of resistance, centred around creating or developing technological tools. With the developments in computation technologies and computer networks, emancipation is possible through developing new software, alternative computer networks or computer systems. It can occur through the utilisation of computer programmes for protection, access, or disturbance. Salient examples include movements like the Cypherpunks, focusing on Strong Encryption, and +KAOS which focuses on alternative data infrastructures. Moreover, it includes a plethora of smaller initiatives and projects, like the open-source InformaCam, which enables editing meta-data of visual content to obstruct surveillance.

In contrast to 'technical counter-surveillance,' other strategies include 'artistic counter-surveillance' where works of art are created as the principal means of countering surveillance. In addition, 'pedagogical counter-surveillance' emphasises education and increasing awareness, while 'legal counter-surveillance' counts on the powers of law.

Despite the promising claims of Technologist Counter Surveillance, the grim reality of today's surveillance/information regime followed the course anticipated and resisted by technologist counter-surveillance advocates. The contemporary surveillance regime has not been overcome–quite the contrary, it has been reinforced. There is, however, a dilemma at the heart of the technologist approach. With its various approaches and complexities, the technologist approach to countering the surveillance regime has been a disturbing force causing ameliorative outcomes–including leaks about human right violations and institutional corruption, disturbing colonial narratives, as well as developing privacy-oriented computer software, hardware and networks which is of a critical emancipatory role. Yet simultaneously, its practices and imaginaries are an intimate part of the information regime they seek to overcome. At times they have reinforced power relations of domination and at other times they have been forces of emancipation. This dilemma is the concern of this paper.

This article investigates the Cypherpunks as an example *par excellence* of the technologist approach to counter-surveillance. After all, the Cypherpunks 'write code'. Importantly, the continued global influence of the Cypherpunks places the group at a central position in the scene of 'technologist resistance',

as "perhaps the single most effective grassroots organization in history dedicated to protecting freedom in cyberspace" (Beltramini, 2021, 101). The geographical location bestowed the Cypherpunks with a rare opportunity– they emerged at a critical juncture of historical, economic and technological developments in the US and without any rivals capable of countering this technologist narrative (Barbrook & Cameroon, 2001).

Nevertheless, to understand this dilemma and the Cypherpunks, it is necessary to locate them in relation to a theoretical understanding of the regime within/against which they operate. This paper locates the Cypherpunks vis a vis the *information regime* as a form of *control* operating according to the imperatives and dynamic of *psychopolitics*–as proposed by Byung-Chul Han. By so doing, this paper attempts to demonstrate the following: Technologist counter-surveillance takes place necessarily *within* the information regime, which is the same regime it tries to counter. It is of a dual character: at once disruptive of, and reinforcing the information regime.

The Information Regime and Psychopolitics

Han starts with an observation of a crisis—the '*crisis of freedom*'. In the information regime, freedom is exploited for economic gains. He states that: "In actual fact, freedom represents the antitype of compulsion—period. And yet this same antitype is now bringing forth compulsion and constraint. More freedom amounts to more pressure." (Han, 2017b, 48-9).

Han concurs with Deleuze (1992) on the emergence of a new form of power–the '*society of control*'. It is a mutation from the '*society of disciplines*' of the industrial era. Foucault (1978) speaks of a transformation from 'sovereign power' to 'biopolitical power'. The former operated by means of deduction and seizure (the sovereign has the right to 'take' life and 'let' live). Biopolitical power, however, operated by 'disciplines'. *It targets bodies*. The bodies of both the individual (anatomo-politics of the human body) and species (biopolitics of population). Rather than 'deduction', it seeks to administer life; to 'invest' it. Here, 'disciplines' ensure the production of the 'docile body', to be useful for efficient production. It brings life into the realm of explicit calculation. This transition into new '*technologies of power*' was necessary for the development of capitalism. "[Capitalism] would not have been possible without the controlled insertion of bodies into the machinery of production and the adjustment of the phenomena of population to economic processes." (Foucault, 1978, 141).

The society of disciplines operates through enclosures; i.e. institutions. The exemplary model is the factory. Institutions are discrete, discontinuous. Here, the subject is cast into a 'mold', moving from one enclosure to another, for the purpose of efficient management. Deleuze (1992) speaks of a crisis of institutions, referring to the emergence of a regime operating through 'modulation' rather than 'molds'–the society of control. The mold is ever self-deforming, continuously in change and re-molding. Instead of factories we have corporations. *Control* is not finite, discrete and discontinuous. Unlike disciplines, it is continuous and limitless, of short-term and rapid rates of change. This transformation arises again to increase efficiency in the immaterial, networked, post-industrial mode of production in the information age, and to overcome the limitations for production. Here, instead of being molded, the subject is made "amorphous, shapeless, and flexible, an adaptive and self-starting entrepreneur" (Wyllie, 2024, 18). Rather than biopolitics, we have Psychopolitics (Han, 2017b), which *targets the Psyche*.

Han brings another important insight. Later, Foucault begins to focus his analyses on 'arts of existence', or '*technologies of the self*'–that is, the techniques individuals deploy to transform themselves in accordance with certain values and criteria. Indeed, 'technologies of the self' are inseparable from the effects of the 'technologies of power'. Disciplines and norms impact on how the subject seeks to act upon itself. Nevertheless, intentionality and voluntarity are of significance in this context (Foucault ,1985, 1988).

Han's main critique of Foucault lies here. He states that Foucault "did not see that *the neoliberal regime utterly claims the technology of the self for its own purposes*: perpetual self- optimization" (2017a, 28, italicised in the original). In other words, the neoliberal regime renders the technologies of the self into technologies of power. Hegemony and coercion coincide. The 'intentionality and voluntarity' are being exploited through psychopolitics, on the pre-reflexive, unconscious level. For Han, it is in this framework that the 'crisis of freedom' emerges.

Furthermore, each society has associated with it certain types of machines, which expresses (not determines) the social forms which generate and utilise them–here, computers (Deleuze, 1992). Psychopolitics enables and is dependent on the digital paradigm, so much as the latter depends on it (Han, 2017b, 2022).

Han calls the digital paradigm the '*information regime*'. It refers to a novel form of domination in which the decisive influence on the social, political and economic fields is exerted by information—that is, through the collection,

storing, and processing of data (Han, 2022). What defines power here is not necessarily the owning of the means of production, rather the ownership of, and capabilities to access, retain, and process data. The information regime is intimately tied to *information capitalism*, which is the intensified development, mutation of capitalism under neoliberalism. Under the information regime, communication and control coincide to become one and the same (Han, 2017a). "Surveillance and control represent inherent features of digital communication" (Han, 2017b, 72), all for the purposes of the *datafication* of social life. Datafication produces and perpetuates the imperative of *Transparency*. Transparency refers to 'the' systematic compulsion to give and circulate information with acceleration, since everything is to be transformed into information and communication. The information society is a society of transparency. It works along the imperative of positivity, by force turning everything into information. Transparency is required under the demands of the freedom of information and the freedom of circulation (Han, 2015a, 2017a, 2022).

A second Enlightenment emerges. In the disciplinary society, Statistics was the mode of calculation, celebrated as a revolutionary force. In the information regime, however, '*dataism*' is the new faith. Its dispositive: all is to be rendered information. It fetishizes data. Everything that can be quantified, should be quantified. In addition, ideology and theory should be rendered obsolete (Han, 2017a, 2022). "[E]verything that can be measured should be measured; that data is a transparent and reliable lens that allows us to filter out emotionalism and ideology; that data will help us do remarkable things — like foretell [sic.] the future." (Brooks, 2013). Datafication and dataism have become accepted scientific paradigms for understanding social behaviour and relationships. Dataism, however, relies on problematic ontological epistemological claims: mainly, that data is objective and raw (van Dijk, 2014).

Knowledge here relies on correlation, which is the most primitive level of understanding. It represents probability and ignores causality, conceptual reciprocity, and 'Concepts', which provides a complete comprehension of the correlation in question. As such, "*Totalized data-knowledge amounts to absolute ignorance*" (Han, 2017a, 70, emphasised in original). Dataism and its transparency dispositif herald a false clarity. It is an ideology that "uses the aura of science to perpetuate the idea that its abstract mathematical models provide a reliable way of knowing, and promotes a reductive definition of truth that is claimed as inherently superior to lived experience" (McQuillan, 2022, 51).

Hans' analysis links up with Lyon's concept of surveillance culture (Stoneman, 2024). Lyon (2017, 2019) observes the emergence of an unprecedented culture regarding surveillance. He uses 'surveillance culture' to explain two phenomena. The first concerns the widespread compliance with surveillance, the second concerns the fact that people not only engage with surveillance, but also initiate it. It is in this context, for Lyon, that people are conditioned to voluntarily hand out data and private information.

While Han's analyses overlap with Lyon's, Han observes a more fundamental social transformation. He understands these phenomena through the shift to psychopolitics. Two elements are important in his analyses: '*emotional capitalism*' and '*gamification of life*'. Here, a tension between rationality and emotions is at play. Han notices a sudden boom of interest in emotions that erupts primarily from an economic process.

In *Emotional capitalism*, "[t]he neoliberal regime deploys emotions as resources in order to bring about heightened productivity and achievement" (Han, 2017a, 45). Emotions are nowadays more consumed than any other goods or services, and can be consumed on end. Emotions, thus, transcend value in relation to consumption. This is at the heart of the crisis of freedom. To 'function,' the docile body of disciplines needed to be an 'unfeeling machine'. In psychopolitics, emotions are elicited and hailed as the expression of the liberated subjectivity. Emotions are 'raw materials' exploited for the purpose of corporate optimisation. To understand this, it is important to consider the distinction between two responsive elements the Pysche characterised by opposing temoporalities and intentionalities; namely, emotions and feelings. Unlike feeling, emotions are short-lived and fleeting, they are dynamic and performative–directed towards action. Moreover, Emotionality is the opposite of rationality. It is characterised by subjectivity, situatedness and volatility. It prefers change and shifts in perception. It demands acceleration.

Emotional capitalism exploits the dynamism and performativity of emotions, enabling the acceleration of communication and the circulation of information. Emotions are, thus, elicited and encouraged along the line of transparency and positivity, perpetuating the illusion of the free subject. It is through emotional capitalism, that the information regime is able to modulate the psyche and render it exploitable.

Another issue is the *gamification of life*. It is not simply a matter of seriousness and leisure becoming one and the same. It is a matter of broadening the scope of the exploitable. Gaming is the 'other' of work. It operates with a temporality

characterised by an instant sense of reward, delivering an immediate experience of success. This, in turn, delivers higher performance, and stimulates further motivation—emotions. The *homo ludens* (man the player) is being emotionally invested, made to work in a manner that surpasses the way the *homo laborens* (man the worker) engages with/in labour. Life and Work become gamified to the end of increasing productivity, *rendering the totality of life exploitable*.

This produces a form of 'smart power', along the dictates of positivity. Unlike disciplines, control works by seducing, inciting and encouraging the subject. It encourages self-illumination and self-exposure. It thrives on auto-exposure. As such, this form of power is so efficient, manipulative and imperceptible (Han, 2017a, 2017b, 2022). Furthermore, psychological maladies ensue, impacting the resisting agent and undermining the potential for efficacious collective action. The positivity of the achievement society de-interiorises the subject and its capacity for reflection by stripping it out of the negativity necessary for reflection and action; for negativity, otherness and foreignness hinder the acceleration of communication and information circulation.

Negativity (along with positivity) is inherent in thinking, as the latter depends on discerning, selection and distinguishing. Reflection adheres to a different temporality–it is slow, engaging in selection, affirmation and exclusion. As such, it is capable of producing alternative ways of life and programmes for moving forward and questioning power (Han, 2015b, 2017b, 2022). The absence of negativity and reducing knowledge to correlation, result in communication without a community. It renders discourse 'superfluous' and the public sphere dismantled; making the potential for collective action unlikely. In the contemporary digital sphere, content creators and followers do not constitute a public sphere, rather, they are more akin to 'swarms'—gathering of fleeting patterns, volatile and ludic. A swarm is soulless, without a possible political 'we' within it (Han, 2022, Han, 2017b). They exist as digital tribes, rendered commodifiable and lacking the capability to act, but of creating 'shitstorms' (Han, 2017b, 2022).

The Cypherpunks

As the earlier discussion shows, the digital turn brought about a novel form of control, which was perfected through the advanced developments in the fields of Big Data and computational algorithms. Yet the perfection of a regime of domination does not preclude forms of resistance–resistance is a corollary of control. This section investigates the Cypherpunks as a form of Technologist counter-surveillance, before presenting the conclusion of this paper.

A Counter-Surveillance Force

One hundred and forty years after the 'Communist Manifesto', another haunting spectre is declared. "A specter is haunting the modern world, the specter of crypto anarchy." (May, 1988). In 'The Crypto Anarchist Manifesto,' Timothy C. May (generally considered the brain of the Cypherpunks) foresees an inevitable total anonymity ensuing the developments in strong cryptography. It will transform the nature of governmental regulations and economic interactions, rendering interference in individual and economic life largely, if not at all, obsolete. This was the motivating spirit and the core of the vision of the Cypherpunks and groups influenced by them. The Cypherpunks were founded in Silicon Valley in 1992 by Timothy C. May with Eric Hughes and John Gilmore. A group of 16 people started gathering every Saturday in an area for tech start-ups. Shortly, an unmoderated, free, and anonymous mailing list emerged, attracting hundreds of global participants in a few years.

The Cypherpunks envisioned four strategic goals. The first, primary, goal concerns free access to cryptographic technologies. Two other goals are anonymous communication and economic interactions free from interference. Finally, developing whistleblowing and leaking platforms to reduce the institutional power (Jarvis, 2021). The following discussion demonstrates the dynamics and thoughts of the Cypherpunks, utilising two issues that are also still relevant today; namely, whistleblowing and cryptocurrencies.

Whistleblowing refers to the act of an insider publicly exposing organisational secrets. Digital technologies afforded whistleblowing unprecedented reach, volume and impact. The Cypherpunks realised this since the early days of computers, as a central strategy against technological authoritarianism. Wikileaks and Julian Assange (a cypherpunk) are an exemplary case to the impact of whistleblowing.

A long-established idea among the Cypherpunks is that technology will (potentially) facilitate a constant, grandiose stream of leaking and whistleblowing. It was a desirable and essential strategy to weaken centralised authorities and interference. Strong encryption technologies and anonymous systems should be developed partly to encourage and facilitate such leaks from within organisational structures. Strong Cryptography is an assurance against exposure and retaliation as well as for obtaining reliable knowledge about institutions.

About the time of releasing the first leak, Assange (2006a) published 'Conspiracy as Governance.' Conspiracy is "the primary planning methodology behind

maintaining or strengthening authoritarian power" (02). Like a network it is greater than the sum of its nodes, as both a functional and cognitive device. The aim is to understand its structure, cleave or throttle it *ad infinitum* so as to reduce its 'total conspiratorial power.' Alternatively, it should be deceived and blinded so as to distort its outcome, to ultimately disable its 'conspiratorial cognitive abilities.' Later, Assange (2006b) contends that the more secretive an institution, the higher the 'secrecy tax' it has to pay. Leaks would lead to 'consequent system-wide cognitive decline resulting in decreased ability to hold onto power as the environment demands adaption [sic.]' (2006b). In line with the legacy and the vision of the Cypherpunks, he adds: "Hence in a world where leaking is easy, secretive or unjust systems are non-linearly hit relative to open, just systems…mass leaking leaves them exquisitely vulnerable to those who seek to replace them with more open forms of governance" (2006b, n.d.).

It is a long standing theme for Cypherpunks. For example, May proposed the use of Cryptographic technology for whistleblowing as early as 1988, as a principal cryptographic application. The platform 'alt.whisteblowers.' was the first such application. Whistleblowing symbolizes the imaginaries, tactics and strategies of the Cypherpunks. Moreover, whistleblowing is an essential tactic in their strategy of 'Diffusion, Confusion, and Refusion.' It is a process of resistance to be employed *en masse*, and in combination with other tactics and activities. It is meant to be an antidote for shutting down this alternative, dispersed system.

In addition, it is an essential part in the strategy for the ideal open society which will become possible (and inevitable) in the digital age. The ideal driving this society is the motto "privacy for the weak, transparency for the powerful." (Assange et al., 2012, 07). Privacy, for the Cypherpunks, is understood as 'the power to selectively reveal oneself to the world' (Hughes, 1993, n.d.). People can retain memories of their interactions while revealing as little as possible, at their will. This is antithetical to a system of surveillance, where one must always reveal themselves–the transparency imperative. And in this open society, *faceless* organizations should never be entrusted with our privacy (ibid).

Furthermore, the idea of *dispersion* is central to the vision of the Cypherpunks. It is the effective approach against 'technocracy' as a centralised, hierarchical system. Dispersion characterises the alternative technological system they envision, and the modus operandi in the open society. In the words of May,

"Cypherpunks know that a widely dispersed system can't be shut down." (May, 1994a, n.d.). In "A Cypherpunks Manifesto", Hughes stresses the indestructibility of software that is capable of moving beyond borders and jurisdictions. Such a system is powerful because it is so widely distributed freely among individuals and software developers, who further develop the capabilities of the software.

Privacy, however, can be effectively applied only if everyone is using strong cryptographic technologies. In a crypto-anarchist society "*everyone* should learn enough to at least vaguely understand how 'blinding' [the surveillance regime] works" (May, 1994a, n.d.; emphasis added). This concept animates many of the technologies developed or advocated for by the Cypherpunks, like Blockchain and Onion Routing technologies as well as virtual communities. Indeed, central to the Cypherpunks anti-hierarchy, but here the element of dispersion becomes a mode of resistance and struggle (May, 1994a, n.d.).

Cryptocurrencies are another central issue. Anonymous economic transactions are a primary objective of the Cypherpunks, demonstrating some of their central concerns and positions such as anonymity and decentralisation.

The problem of digital cash goes back to the 1980s, pioneered by David Chaum, who developed the first digital monetary systems. Unlike Chaum's digital currencies, Bitcoin enabled decentralisation for the first time; a truly distributed system. As for anonymity, it is a hybrid system–account holders are anonymous while the transactions are completely public. Trust is distributed and enforcement is not descending from a regulating body. Rather, trust and enforcement emerge from mathematics and technology–through the difficulty of cryptographic and mathematical computation required for the creation and transaction of a bitcoin, in which every part of the network is engaged as a manner of proof (the Blockchain) (Assange, in Assange et al., 2012). Anonymity can be increased by utilising other technologies like Onion Routing (Hidden Services) or I2P. All in all, "Bitcoin was the most successful attempt to introduce a digital currency for the last ten years" (Muller-Maguhn, in Assange et al., 2012, 99) and it is a step in the right direction in relation to privacy for everyone (Appelbaum, in Assange 2012, 100).

In this context, a relevant issue for 'throttling' technocracy is taxation–a central concern of the Cypherpunks. Tax evasion is deemed an effective strategy to minimize state interference in economic interactions; accompanied with underground economies that are both inevitable and desirable. It can

inhibit the emergence of a surveillance regime, as an antidote to the state's raising taxes and as a haven for money to eventually escape the grip of the state (Ludlow, 2001).

These positions can be challenged. These are, however, the imaginaries and practices of the Cypherpunks–the concern of this paper. The importance of these issues stem from a central concern of the Cypherpunks. They emphasised a central shift in the regime of power accompanying the digital turn (Beltramini, 2021). Power has become manipulative and imperceptible, operating as a system of control through surveillance. Power has become a totalising 'smart power'. Hence the significance of such alternative technologies. Thus, they proposed a holistic approach to counter technologist authoritarianism, not simply a set of technological tools. While euphoric about the promises of technology, it is a significant opposition to the information regime. *It starkly opposes dataism and the transparency dispositif*. Moreover, *it seeks to inverse the power asymmetry surrounding privacy*: privacy for the weak, transparency for the powerful. Nevertheless, the imaginaries of the Cypherpunks and their impact as to the emergence of the information regime brings up again the dilemma at the centre of this article.

A Force for the Information Regime

The Information regime brings about a crisis of freedom, which is central to the Cypherpunks. It is however a contested concept within the group–which is of a great variety in terms of individuals' background and ideological inclinations. Freedom, thus, is a plausible entry point here. A question arises as to whether they are concerned exactly with freedom or with the crisis of freedom. This has implications for understanding their broader ideological position. An established position is that the Cypherpunks are libertarian or anarchist (Jarvis, 2021).

Beltramini (2021) challenges this established position. According to him, the Cypherpunks were first and foremost against the regime of technocracy (technocratic authoritarianism). Their central struggle revolved around the "crisis of freedom," rather than freedom per se. In other words, the problem for crypto-anarchists was not the state per se, rather with the state becoming an apparatus within an extensive network of social control and domination. The implementation of the state is the problem rather than the state itself, and the remedy comes from technology, not law–for the democratic system has become broken. This is a necessary consequence resulting from the trajectory of modernisation, or the societies of affluence and post-industrialism. It is

not a political anarchism, rather an anarchism of cyberspace, emerging out of a "mix of nihilism and protest, anger and radicalism, disillusion and vitriol, scepticism and resistance and uncompromising opposition" (ibid., 111). Cryptographic tools allowed the perception of the possibility of bringing about some anarchist ideals (Ludlow, 2001). However, this association between anarchism and the Cypherpunks might be due to anarchism's lacks a unitary definition, conceived by its proponents as an ethical standpoint (Franks et al., 2018), to a misconception that the central theme of anarchism is the rejection of state (Amster, 2018) and that liberty is the determining value of anarchist political philosophy (May, 2008).

But here arises a question as to the nature of this 'freedom' for the Cypherpunks. Hellegren (2017) points out that the principal issue in this 'discourse community' is particularly *'internet' freedom*. Importantly, crypto-discourse in general emphasises a negative concept of freedom. This negative conception of freedom removes the responsibility from states and lays it on the shoulders of individuals–if they wish to protect themselves from surveillance and to practice their freedom of speech. This stance is rooted in the liberalism found in the United States (Coleman & Golub, 2008). By excluding positive conceptions of internet freedom, this discourse deepens the democratic deficit.

The only unifying element in the Cypherpunks, is their Technologist position–their belief that technology and strong cryptographic tools is the primary way for (internet) freedom. Nevertheless, "Crypto-advocates have over time emptied crypto of its particular meaning and filled it with multiple possible meanings that unite different political objectives through the construction of a social antagonism" (Hellegren, 2017, 290). They are only unified through the discursive practices governing the meaning-making processes with these communities.

For Coleman and Golub (2008) the internet is "a privileged site for projecting the aspirations of liberal society." (270), where Crypto-anarchy is a particular moral genre. Liberalism here is a cultural sensibility, not a coherent body of thought. They are one manifestation of the liberal *'expressive self'*. Computer hacking is a location wherein liberalism is not only manifested but also wherein its commitments and critiques are articulated and transformed, in a dialogical and heterogeneous manner, with/as a set of historical, moral and cultural sensibilities. This now takes place with technical parlance and "is given new life and visibility in the digital age." (258). The 'expressive self' is realised by 'writing code' (as per Hughes; 1993). The Cypherpunks, thus, represent

the general American liberal sensibility, in a technologist manifestation. The suspicion they hold towards the state is located here and can be equally seen as within libertarian right as well as within the anti-military left pacifism. Nevertheless, they do not adopt any clear political affiliation, and many among them think of their projects as continuation and affirmation of cultural and constitutional principles inherited from earlier times.

This notwithstanding, there is an oscillation between negative and positive notions of freedom, in addition to a tension between individualism and collectivism–which are both tensions that can be traced back in the tradition of liberalism itself and its cultural context, particularly in relation to freedom. This brings up two issues: The Californian Ideology and the mode of operation of the Cypherpunks as a 'collectivity'. The Cypherpunks might be better understood if placed in the context of a particular subculture, rather than the broader American or ideological contexts. The first link between crypto-anarchism and libertarianism was first publicly established in the second issue of the renowned WIRED technology-focused magazine (Issue 1.02 of May/ June 1993)–featuring the founders of the Cypherpunks as "Rebels with a Cause (Your Privacy)". The Magazine was "the monthly bible of the 'virtual class'" (Barbrook & Cameron, 2001, 368).

The Californian Ideology was advocated by the digerati (digital literati) and the virtual class. It has dominated the technology scene in the United States and beyond. Prominent ideologues included Kevin Kelly, Douglas Rushkoff, Lou Rossetto, and John Perry Barlow. For them, technology enables life to move beyond the confines of evolution, making humanity superior. This vision can be traced back to the ideas of Ecosystems and cybernetics (Curtis, 2011). The avant-guards of such development are none but the digerati themselves, the collection of the boundless get-it-alone individuals, the ultra-individualists, who would 'advance civilisation' (Purdy, 1998). Life is nothing but a self-ordering and self-reproducing system, with feedback loops, consisting of vivisystems, driven by an invisible hand with a spontaneous order–which should not be interfered with. Computers, like humans, are vivi-systems. The task for humanity is to facilitate and extend the passing of life to the new vivi-system–since only humans are the vivi-system capable of doing so (ibid.).

For this, the digerati are uninterested in politics and social life (except when it concerns cyber interests). They are insignificant, considering the larger landscape and dynamics of Life. For Purdy, they are post-humanist vitalists. The individual is a supermensch–a boundless individual who can change things

at will. “Wired is about the most powerful people on the planet today—the Digital Generation.” (Wired’s first issue, 1993, cited in ibid.). They overlook the intricacies of life, with its political, economic, and social dilemmas and troubles, favouring the celebration of Life, as envisaged by them. The problem with the state, for them, is its interference in this spontaneous order. “[I]n place of counterproductive regulations, visionary engineers are inventing the tools needed to create a “free market” within cyberspace, such as encryption, digital money, and verification procedures” (Barbrook&Cameron, 2001, 369).

Important is the discussion as to the question of equality. This also concerns an important tension about freedom and equality (May, 2008), which positions the Cypherpunks ideologically outside anarchism. The digerati are a tribe seeking comradeship among equals, who are wilfully ignorant and negligent of others–due to their negligence of the limitations of life. These others are, however, the groups most affected and harmed by the new technologies and discourses. It is a complacency that is deeply rooted in, and not just a by-product of this line of thought and temperament. This necessarily leads them to over-emphasise their assumptions as universal, at the expense of others. In addition, the digerati are oblivious to the fact that their environment and doctrinal documents are largely produced by white men and dominated by big technological corporations–leading them to such meaningless and undesirable grim utopias. As such, theirs is a vitalistic picture of democracy, bordering on mysticism and enmeshed with intellectual pretence and delusions.

Furthermore, this ‘virtual class’ is a form of retrofuturism (Barbrook & Cameron, 2001) that seeks a Jeffersonian democracy, bringing atavistic elements of the American culture, with the pretence of being progressive. Simultaneously, they attempt to combine elements from, and realise the utopias of both the New Left and the New right–without criticality. Advanced technologies would realise the electronic agora and replace big government and corporate capitalism while at the same time empowering the individual to freely interact in the free market, which will advance the progress of technology and lead to democracy. It is a self-contradicting position, possible only with a firm, positive technological determinism. The Californian Ideology reflects their professional reality. They were employed with fixed-term contracts, and despite being well-paid and enjoying a level of autonomy they had no guarantee as to the future of their employment.

This position calls for a democracy in which technologies are in fact created to mediate their interaction with the reality of labour. They claim to be progressive while engaging in the opposite of such claims. This utopian vision creates a

new form of apartheid between the information-rich and the information-poor. The virtual class opt for 'living' in the hyperreality of virtual communities, calling for further immersion in the cyberspatial world, reinforcing the impacts of their wilful blindness and dependence on the Other.

As such, the Cypherpunks are still *within* the information regime. While opposing the technocracy, and the imperatives of psychopolitics, they reinforce some of these imperatives. Their concept of freedom *reinforces the crisis of freedom*, by reinforcing the logic of the entrepreneur self/project and by adopting a *negative concept of freedom* which lays the onus of protection and emancipation on the individual. This concept of freedom, moreover, operates in accordance with the logic of positivity of psychopolitics. This, in turn, results in the lack of negativity necessary for reflection and narrative, further exacerbating the *crisis of narrative*. This leads to the Cypherpunks operating as a *swarm*, rather than a collective movement with a spirit and direction.

Conclusion

Technologist counter-surveillance refers to the approach which emphasises the primacy of developing/altering digital technologies as the principal means and strategy for resisting surveillance. The concern here is with a dilemma at the heart of this phenomenon: while being a disturbing force which caused significant ameliorative outcomes with pivotal emancipatory role, technologist counter-surveillance have also reinforced power relations in the information regime. This paper investigated the Cypherpunks as an exemplary case of Technologist Counter-Surveillance, analysed in the context of the information regime as a form of control operating according to the imperatives and dynamic of psychopolitics.

The paper argues that Technologist counter-surveillance takes place necessarily within the information regime, which is the same regime it tries to counter. It is of a dual character: at once disruptive of, and reinforcing the information regime.

References

Amster, R. (2018). Anti-hierarchy. In B. Franks, N. Jun, & L. Williams (Eds.), *Anarchism: A conceptual approach* (pp. 14–27). Routledge.

Assange J. (2006a). *Conspiracy as Governance*. [Online]. https://estaticos.elmundo.es/documentos/2010/12/01/conspiracies.pdf

Assange J. (2006b, December 31). *The nonlinear effects of leaks on unjust systems of governance*. https://web.archive.org/web/20071020051936/http://iq.org/#Thenonlineareffectsofleaksonunjustsystemsofgovernance

Assange J. et al. (2012) *Cypherpunk: Freedom and the Future of the Internet*. OR Books, New York and London.

Baaz, M., Lilja, M., Schulz, M., & Vinthagen, S. (2023). The ABC of resistance: towards a new analytical framework. *Journal of Political Power*, 16(1), 59-80.

Barbrook, R. & Cameron, A. (2001). Californian Ideology. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (363-387). The MIT Press. England.

Beltramini, E. (2021). Against technocratic authoritarianism: A short intellectual history of the cypherpunk movement. *Internet Histories*, 5(2), 101-118.

Brooks, D. (2013, Feb 4). The philosophy of data. *New York Times*, 4(02). https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html

Coleman, E. G., & Golub, A. (2008). Hacker practice: Moral genres and the cultural articulation of liberalism. *Anthropological Theory*, 8(3), 255-277.

Curtis, A. (Director) (2011). *All watched over by machines of loving grace* [Film]. BBC. London.

Deleuze, G. (1992). Postscript on the Societies of Control. *October*, Vol. 59. (Winter, 1992), pp. 3-7.

Ettlinger, N. (2018). Algorithmic affordances for productive resistance. *Big Data&Society*, 5(1), 205395171877139. https://doi.org/10.1177/2053951718771399

Foucault, M. (1977). *Discipline and Punish: The Birth of the Prison*, trans. A. Sheridan. Vintage.

Foucault, M. (1978). *The History of Sexuality, Volume 1: An Introduction*, trans. R. Hurley. Vintage.

Foucault, M. (1990). *The History of Sexuality, Volume 2: The Use of Pleasure*, trans. R. Hurley. Vintage.

Franks, B., Jun, N., & Williams, L. (2018). Introduction. In Franks, B., Jun, N., & Williams, L. (Eds.). (2018). *Anarchism: A Conceptual Approach* (pp. 1-12). Routledge.

Han, B. C. (2015a). *The transparency society*. Stanford Briefs.

Han, B. C. (2015b). *The burnout society*. Stanford University Press.

Han, B. C. (2017a). *Psychopolitics: Neoliberalism and new technologies of power*. Verso Books.

Han, B. C. (2017b). *In the swarm: Digital prospects*. MIT press.

Han, B. C. (2022). *Infocracy: Digitization and the crisis of democracy*. John Wiley & Sons.

Hellegren, Z. I. (2017). A history of crypto-discourse: Encryption as a site of struggles to define internet freedom. *Internet Histories*, 1(4), 285-311.

Hughes, E. (1993, March 9). *A Cypherpunk's Manifesto*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/library/cypherpunk-manifesto/

Jarvis, C. (2021). Cypherpunk ideology: objectives, profiles, and influences (1992–1998). *Internet Histories*, 6(3), 315-342.

Lilja, M. (2022). The definition of resistance. *Journal of Political Power*, 15(2), 202-220.

Lilja, M., Baaz, M., Schulz, M., & Vinthagen, S. (2017). How resistance encourages resistance: theorizing the nexus between power,'Organised Resistance'and 'Everyday Resistance'. *Journal of Political Power*, 10(1), 40-54.

Ludlow, P. (2001) New Foundations: On the Emergence of Sovereign Cyberstates and Their Governance Structures. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 1-24). The MIT Press. England.

Maxigas (2017). Preface. In Beritelli, L. (2017). + *KAOS: ten years of hacking and media activism* (pp. 11-18). Institute of Network Cultures. Amsterdam

May, T. (2008). *Political Thought of Jacques Rancière: Creating Equality*. Edinburgh University Press.

May, T. C. (1988). *Crypto-Anarchist Manifesto*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/library/crypto-anarchist-manifesto/

May, T. C. (1994a, September 10). *The Cyphernomicon*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/library/cyphernomicon/

May, T. C. (1994b, December). *Crypto Anarchy and Virtual Communities*. Satoshi Nakamoto Institute. https://nakamotoinstitute.org/library/virtual-communities/

McQuillan, D. (2022). *Resisting AI: An anti-fascist approach to artificial intelligence*. Policy Press.

Purdy, J. S. (1998) The God of the Digerati. In Ludlow, Peter (ed.) (2001) *Crypto Anarchy, Cyberstates, and Pirate Utopias* (pp. 353-362). The MIT Press. England.

Sewell, S. A. (2021). Surveillance on the assembly line: Communist resistance to modern production at the Stollwerck Chocolate Factory, 1924–1930. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 87-104). Routledge.

Skare, E. (2016). *Digital Jihad: Palestinian resistance in the digital era*. Bloomsbury Publishing.

Stoneman, E. (2024). Digital Psychopolitics: Towards the Total Control Society. In Knepper, S., Stoneman, E and Wyllie, R. *Byung-Chul Han: A Critical Introduction* (pp. 64-93). Polity. Cambridge.

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveillance & society*, 12(2), 197-208.

Weller, T. (2022). The historical ubiquity of surveillance. In Marklund, A., & Skouvig, L. (2021). *Histories of Surveillance from Antiquity to the Digital Era* (pp. 163-179).

Wyllie, R. (2024). Burnout: Against Achievement Culture. In Knepper, S., Stoneman, E and Wyllie, R. *Byung-Chul Han: A Critical Introduction* (pp. 8-34). Polity. Cambridge.

Yu, Z., Treré, E., & Bonini, T. (2022). The emergence of algorithmic solidarity: Unveiling mutual aid practices and resistance among Chinese delivery workers. *Media International Australia*, 183(1), 107–123. https://doi.org/10.1177/1329878X221074793