The Cypherpunk Vision of Techno-Politics

Maud Barret Bertelloni

The cypherpunk movement emerged out of the convergence of online cryptology discussion groups and a mailing list founded in 1992 by technologists John Gilmore, Timothy May, and Eric Hugues. A year later, Hugues wrote "A Cypherpunk's Manifesto"[1], coining a name that combined the "cypher" prefix, both a reference to cryptography and to the secrecy which it preserves, with "punk", a term with anarchist, anti-authoritarian and generally irreverent connotations.[2] The name echoed May's "Crypto-anarchist Manifesto" presented at the group's first meeting,[3] in which he highlighted the transformative potential of technologies related to cryptography. Throughout the years, the group assembled – online and offline – some of the most important technologists and cyber-activists in the world,[4] forming organizations ranging from the Electronic Frontier Foundation to WikiLeaks, tied to the development of technologies ranging from the onion router Tor to various crypto-currencies.[5] They shared the conviction that their anarchist beliefs were to be implemented through the technologies they developed, the majority of which relied on cryptography. In this sense, the cypherpunk movement can be termed a techno-political movement, because it realises its political aims through technological means.[6]

Although some view "techno-politics" as the political controversies over technological questions, particularly over their accessibility or over the openness of the Internet,[7] the cypherpunk movement seems to take a more expansive view of techno-politics, believing that technology itself, when implemented, is a political tool in its own right and serves to propagate particular values. This echoes Langdon Winner's theory that artefacts have inherent politics, by design,[8] just as networks like the Internet, in Lawrence Lessig's words, are regulated by architecture.[9] But in this case, would it still be possible to distinguish the "aims" from their technical "means"? Wouldn't this techno-political stance

[1] Eric Hugues, "A Cypherpunk's Manifesto", Electronic Frontier Foundation, accessed December 20, 2016, https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto.

[2] Craig O'Hara, *The Philosophy of Punk*, AK Press, Oakland, 1999.

[3] Timothy May, "The Crypto Anarchist Manifesto", Activism.net, accessed December 20, 2016, http://www.activism.net/cypherpunk/crypto-anarchy.html.

[4] Cyberactivists like Julian Assange, founder of Wikileaks, TOR developer Jacob Applebaum and Runa Sandvik, Electronic Frontier Foundation activists.

[5] For instance, Zooko Wilcox O'Hearn, developer of DigiCash and founder of Zcash, Wei-Dai, creator of b-money, Nick Szabo, creator of bit gold.

[6] Terje Rasmussen, 'Techno-politics, Internet Governance and some challenges facing the Internet", Oxford Internet Institute, Research Report 15, October 2007.

[7] Mark Rumold, The Freedom of Information Act and the Fight Against Secret (Surveillance) Law, 55 Santa Clara L. Rev. 161, 2015, cited in Can Kurban, Ismena Pena-Lopez and Maria Haberer, "What is technopolitics? A conceptual scheme for understanding politics in the digital age", Building a European digital space. (paper presented at the 12th International Conference on Internet, Law & Politics at the Universitat Abierta de Catalunya, Barcelona, July 7-8, 2016). Human Enhancement and the emergent technopolitics of the 21st century", in Managing nano-bio-info-cogno innovations, ed. W.B. Bainbridge, Springer, 2006. Cited in Kurban, Pena-Lopez and Haberer.

[8] Langdon Winner, "Do Artifacts Have Politics?", Daedalus 109, n°1, 1989, pp. 121-136.

[9] Lawrence Lessig, "The Laws of Cyberspace", paper presented at the Taiwan Net '98 Conference, Taipei, March 1998.

imply that the implementation of particular technologies in turn imposes particular political values and visions?

Thus, in order to analyse the political beliefs and methods of one of the groups that has accompanied the development of the Net in the past three decades, it is pertinent to ask: What is the relationship between technology and politics in the conception of the techno-politics of the cypherpunk movement? This essay will make use of written sources, notably Eric Hugues' "A Cypherpunk Manifesto"[10] and Timothy May's "The Crypto Anarchist Manifesto,[11] the archives of the cypherpunk mailing list, and analyses of widely circulated software, protocols, methods, and distributed technology, to render the articulation between political and technical views in the cypherpunk conception of techno-politics.

The cypherpunk movement advocates crypto-anarchist political views. The term was coined by Timothy C. May, in the homonymous manifesto, a version of which he read at the cypherpunk founding meeting in September 1992. It consists in a form of anarchy rendered possible by the use of cryptography and its applications.[12] The "crypto" form of anarchism is one that, as May himself later specified, is very distant from Proudhon or Bakunin's anarcho-syndicalism or Kropotkin's communal anarchism: May intends anarchism "in the same sense of anarchy used in anarcho-capitalism, the libertarian free-market ideology that promotes voluntary, uncoerced economic transactions"[13], referring to Hayek and Friedman.

Apart from obvious divergence on the role conferred on the market, another difference resides in different interpretations on the meaning of anarchism, determining its nature. May rashly traces back to the term's etymology, as "literally 'an arch,' without a chief or a head"[14]. It is quite different, however, from the absolute negation of power, as in Proudhon's powerless order. In fact, it is not power that is contested, but its form: anarchy requires "no central control, no ruler, no leader (except by the example or reputation), no 'laws'."[15] Given Lawrence Lessig's thesis that normativity in cyberspace occurs through four instances, these being legislation, social norms, markets and "architecture", it is only the first of these components that crypto-anarchism rejects, for it advocates a free market and ensures social regulation through 'reputation', all this through "code"[16]. In this sense, the type of anarchism that is advocated is close to punk anti-authoritarian, anti-statist currents,[17] with appeal to individual liberty.

These traits allow us to solve the apparent contradiction raised by the proximity of the cypherpunk movement to open source movements.[18] As Applebaum explained in an

[10] Hugues, op. cit.

[11] May, op. Cit.
The Manifesto had previously been presented at the Crytpo Conference in Santa Barbara in 1988.

[12] *Ibid.*

[13] Peter Ludlow, Crypto Anarchy, Cyberstates, and Pirate Utopias, The MIT Press, Cambridge, Massachusetts, 2001.

[14] *Ibid.*

[15] *Ibid.*

[16] Lessig, op. cit.

[17] O'Hara,, op. cit., p. 27-28.

[18] For instance the fact that all source code produced from crypto.is project is open source, or Cypherpunks development of open source versions of technology, like OpenPGP, OpenSSL, etc.

interview, cypherpunk attachment to free software derives from its empowering role: each individual can employ it as a tool for his own freedom.[19] The deployment of cryptography can help oppose governmental influence in anarchist cyberspace and foster individual independence, opposing a "general trend to defer to authority". Technology is for cypherpunks the way to situate the primary source of agency at the level of the individual and this is a vision of techno-politics intended as the potentiation of political aims through technical means.

"Cypherpunks write code": both at personal and systems level, to individual liberty, anti-authoritarianism and free market correspond different applications of cryptography, from implementations of public key encryption, to P2P networks and distributed-ledger-technology-based crypto-currencies. Privacy, for instance, which Erich Hugues defines as "the power to selectively revel oneself to the world" is permitted by public-key cryptography (PKC), which ensures individual protection against state surveillance and censorship. PKC can be used for communications encryption, guaranteeing their anonymity (through plain encryption like PGP or applications like MixMaster remailers).[20] It can also ensure authentication (digital signatures), allowing pseudonymity, setting "persistent" and non-forgeable identities, and bypassing state-assigned ones: they are, in Chaum's words, "credentials without identity"[21] that enable sustained individual action free from any control other than reputation.

Individuals are also at the core of decentralized peer-to-peer networks, participating with their personal devices in tasks that range from running nodes to maintaining networks to hosting files for file sharing. This type of network can be coupled with encryption to ensure, for instance browsing anonymity, like in the case of TOR, the Onion Router. Here, the importance of "architecture" is quite evident: by setting the Internet up as a decentralised system, cypherpunks attempt to secure its lawlessness.

Finally, anonymity and decentralization are coupled in crypto-currencies that run upon DLT. Those rely on cryptographic software protocols to generate the currency and to validate transaction through the verification of the digital signature of payers' public keys, stored on a public distributed ledger operating without central authority on a decentralized network.[22] Cypherpunks were involved in the development of early crypto-currencies,[23] and their mailing lists enabled Satoshi Nakamoto (an example of famous pseudonym) to share his manifesto, "Bitcoin: A Peer-to-Peer Eletronic Cash System". Although studies have indicated that Bitcoin might be de-anonymized,[24] its deployment has facilitated the

[19] Julian Assange, Cypherpunk, OR Books, New York, 2012, p. 42.
Another analogy with punk attachment to "DIY", fostering individual independence.
See O'Hara, *op. cit.*

[20] Mixmaster remailer was developed by Lance Cottrel, another member of the cypherpunk mailing list, using the chaumian concept of mix networks.

[21] David L. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete", Communications of the ACM, vol 28, n 10, 1985.

[22] This ledger another analogy with Chaum's "roster" described in David L. Chaum, "Untraceable Electronic Cash", paper presented at the Crypto '88 Conference. Blockchain in the case of Bitcoin but term has become a general term to refer to distributed ledger technology.

[23] See above.

[24] Androulaki et al. "Evaluating User Privacy in Bitcoin", presented at the International Conference on Financial Cryptography and Data Security, 2013.

emergence of unregulated parallel markets, including money-laundering circuits and illegal markets.[25] Cypherpunk advocates are aware of these dangers, but perceive them as outweighed by the benefits of the elimination of state monopoly over the currency and of its control over markets. May, for instance, wrote that "crypto-anarchy (...) will allow illicit and stolen materials to be traded"; it "will even make possible abhorrent markets for assassinations and extortions[26]". But "just as the technology of printing altered and reduced the power of medieval guilds and the social power structure, so too will cryptologic methods fundamentally alter the nature of corporations and of government interference in economic transactions"[27], overriding concerns with an element of teleology.

Cypherpunks therefore do not only rely on technological artefacts, namely on cryptography and its applications, to potentiate their political beliefs; they also confide in their inalterable properties. Technology is not only a tool, or rather a weapon to fight the "crypto-war" that cypherpunks fight against any government attempting to extend its sovereignty over the cyberspace.[28] The analogy between cryptography and weapons finds echoes in David Friedman's analogy between individual capacity to use encryption and the constitutional right to bear arms granted by the 2nd Amendment in the American Constitution; in this sense "the continuation of politics through other means" could well mean technological ones.[29] This technology, however, is more than a neutral tool – it is held to possess intrinsic properties, which materialise when deployed. This conception, inferred from systems theory is, according to Turner, recurrent in the "cyberculture" in which the cryptography originated.[30] Just as Marshall McLuhan famously stated that "the medium is the message", Phil Zimmerman hoped that PGP would spread "like dandelion seeds"[31] to defeat attempts of state control on cryptography, because its diffusion, regardless of the intentions of its users, would suffice to ensure its success.

Here, however, the belief that technical artefacts have inherent political qualities could entail two types of consequences: either that "certain kinds of technology are unavoidably linked to particular institutionalized patterns of power and authority", or that "features in design and arrangement of a device or system [provide] convenient means of establishing patterns of power and authority in a given setting".[32] Cypherpunks seem to support the latter: May talks about the "technological inevitability" of the inalterable mathematical properties of prime numbers cryptography is based upon. This highlights the clear preponderance of technique over politics, whose scope, in this vision of techno-politics, is very restricted. It isn't quite clear, however, how this natural property actually translates at the level of application, let alone for a whole society: despite the unitary principle of blockchain, for instance, there have been forks deriving from disagreements

[25] Nicolas Christin, "Traveling the Silk Road: A measurement analysis of large anonymous online marketplace", INI/CyLab working paper, November 2012.
[26] Timothy May in Ludlow, op. cit., p. 26.
[27] *Ibid.*
[28] 'The Crypto Wars: Governments Working to Undermine Encryption", Electronic Frontier Foundation, accessed January 1, 2017: https://www.eff.org/document/crypto-wars-governments-working-undermine-encryption.
[29] David D. Friedman, Future Imperfect, Cambridge University Press, Cambridge, 2008, p. 41.
[30] Fred Turner, From Counterculture to Cyberculture, The University of Chicago Press, Chicago, 2006.
[31] Andy Greenberg, This machine kills secrets, Penguin, London, 2011.
[32] Winner, *op. cit.*

over "block size debate".[33] Some crypto-currencies have set up internal governing bodies (RSC coin) and there is no evidence of the ineluctability of the development of an anarchist decentralised society through the deployment of cryptography. The first interpretation, which appears more insightful, would claim that, in line with Lawrence Lessig's words, it is true that different architectures of software and hardware determine how people interact, or exist, in cyberspace, and reflect different philosophies about access, carrying political values. They are in this sense inherently political, but they can also be altered: it is an error of naturalism to believe that some architecture "will guarantee us freedom; that it will of necessity disable governments that want to control."[34] Features in design do entail the establishment of patterns of power and authority in a given setting, but this is by no means an automatic task.

What isn't sure either is whether technology will be a tool for individual empowerment, or at least, for the empowerment of all individuals. May again explains that with the deployment of cryptography, "something that is inevitable is the increased role of individuals, leading to a new kind of elitism. Those who are comfortable with the tools described here can avoid the restrictions and taxes others cannot." Technology, clearly, is tailored for those who master and design it, and so is the cypherpunk cyberspace. This trait of the cypherpunk vision can be explained historically by the fact that in the context of development of cryptography, forms of deliberation other than "rough consensus and running code"[35] were not necessary, so long as the political self-identity of users and creators "belonged to the same equal and limited circle".[36] However, the change in context tied to the privatization of the Internet and its subsequent mass deployment has brought about a great variety of new problems and views concerning the way the Net should be run. The fact that problems of political participation are not contemplated in the cypherpunk vision can help explain why debates over the Internet and cryptography have been so confrontational: from the "crypto-wars" to the "Declaration of Independence of Cyberspace",[37] regardless of the intentions of the parties, teleological accounts of the impact of technology on politics leave little room for alternative stances, other than the goodwill of the technologists.

Cypherpunk techno-politics rely on technology to realize anarcho-capitalism in cyberspace, and technology is intended as more than a mere tool for political aims. Through PKC and its applications, the deployment of decentralised networks and the establishment on crypto-markets online, cypherpunks strive to emancipate the cyber realm from the interference of centralised power structures, and to confer to individuals the sole base of agency. Technology, in this sense, as embedded in artefacts design and network architecture, is considered as the inalterable carrier of particular patterns of power and authority, subordinating other political activities to a teleological and technicist vision of techno-politics, the consequences of which ought to be taken under account in the examination of the past and future development of the Internet.

[33] Grace Caffyn, "What is the Bitcoin Block Size Debate and Why Does it Matter?", Coindesk, accessed January 5, 2017: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/.

[34] Lessig, *op. cit.*

[35] These words, attributed to David Clark, are held to be the motto of the IETF.

[36] Rasmussen, *op. cit.*

[37] John Perry Barlow, "A Declaration of Independence of Cyberspace", Electronic Frontier Foundation, accessed on January 5, 2017: https://www.eff.org/cyberspace-independence.

Bibliography

Primary sources

Books

Julian Assange, *Cypherpunk*, OR Books, New York, 2012.
David D. Friedman, *Future Imperfect*, Cambridge University Press, Cambridge, 2008.
Andy Greenberg, *This machine kills secrets*, Penguin, London, 2011.

Articles

John Perry Barlow, “A Declaration of Independence of Cyberspace”, Electronic Frontier Foundation, accessed on January 5, 2017: https://www.eff.org/cyberspace-independence.
David L. Chaum, “Security without Identification: Transaction Systems to Make Big Brother Obsolete”,Communications of the ACM, vol 28, n 10, 1985.
Eric Hugues, “A Cypherpunk’s Manifesto”, Electronic Frontier Foundation, accessed December 20, 2016, https://w2.eff.org/Privacy/Crypto/Crypto_misc/cypherpunk.manifesto.
Timothy May, “The Crypto Anarchist Manifesto”, Activism.net, accessed December 20, 2016, http://www.activism.net/cypherpunk/crypto-anarchy.html.

Secondary sources

Books

Peter Ludlow, *Crypto Anarchy, Cyberstates, and Pirate Utopias*, The MIT Press, Cambridge, Massachusetts, 2001.
Craig O’Hara, *The Philosophy of Punk*, AK Press, Oakland, 1999.
Fred Turner, *From Counterculture to Cyberculture*, The University of Chicago Press, Chicago, 2006.

Articles

Androulaki et al. “Evaluating User Privacy in Bitcoin”, presented at the International Conference on Financial Cryptography and Data Security, 2013.
Grace Caffyn, “What is the Bitcoin Block Size Debate and Why Does it Matter?”, Coindesk, accessed January 5, 2017: http://www.coindesk.com/what-is-the-bitcoin-block-size-debate-and-why-does-it-matter/.
Nicolas Christin, “Traveling the Silk Road: A measurement analysis of large anonymous online marketplace”, INI/CyLab working paper, November 2012.
Mark Rumold, The Freedom of Information Act and the Fight Against Secret (Surveillance) Law, 55 Santa Clara L. Rev. 161, 2015.
Can Kurban, Ismena Pena-Lopez and Maria Haberer, “What is technopolitics? A conceptual scheme for understanding politics in the digital age”, Building a European digital space. (paper presented at the 12th International Conference on Internet, Law & Politics at the Universitat Abierta de Catalunya, Barcelona, July 7-8, 2016). Human Enhancement and the emergent technopolitics of the 21st century”, in Managing nano-bio-info-cogno innovations, ed. W.B. Bainbridge, Springer, 2006. Cited in Kurban, Pena-Lopez and Haberer.
Lawrence Lessig, “The Laws of Cyberspace”, paper presented at the Taiwan Net ‘98 Conference, Taipei, March 1998.
Terje Rasmussen, ‘Techno-politics, Internet Governance and some challenges facing the Internet”, Oxford Internet Institute, Research Report 15, October 2007.
Langdon Winner, “Do Artifacts Have Politics?”, Daedalus 109, n°1, 1989, pp. 121-136.