CON
CRE
TA

ABOUT CONCRETA | JOURNAL | BOOKS | ONLINE | NEWS | SHOP | SUBSCRIPTIONS

Critique of Software Violence

Geoff Cox   Share

There is an inherent violence of software. Our network operations are dominated by violent acts against us in the form of viruses, spam, phishing, and botnets, and more to point violence is encoded in software itself. [1] Like language, we enter informational infrastructures antagonistically – echoing Judith Butler's observation that we come into language antagonistically from our beginnings. [2] Butler's point is that violence is embodied in language, not simply in the way it might be used to incite a violent action or in the ways that language reflects social domination more generally - such that it can be injurious as in the case of hate speech. But, as Slavoj Žižek has also pointed out, it also is violent in the way that it produces meaning. There is something inherently violent in the capacity of language to represent a thing, what he calls "its essencing ability", equivalent to its symbolic death. As it stands in for something, "it dismembers the thing, destroying its organic unity", and forces the thing into a field of meaning that is outside of itself. [3] This also happens at the level of software, and perhaps in a more overt manner, as programming languages extend natural languages through their protocological address to humans and machines. With program code, it not only symbolizes but enacts violence on the thing: it *executes* it.

But before discussing this operational aspect with respect to software, I will introducethe tricky subject of violence in more detail.As is probably clear at this point, the title of this essay refers explicitly to Walter Benjamin's 1921 essay "Critique of Violence". [4] For Benjamin, at issue is not whether violence is a means to a just or unjust end but whether violence can be a moral means in itself. As he puts it, "a more exact criterion is needed, which would discriminate within the sphere of means themselves, without regard for the ends they serve". So rather than simply reconciling just ends by a justification of the means, or vice versa, the focus is "the question of the justification of certain means that constitute violence". [5] As far as the state is concerned, violence exercised by individuals, or its legal subjects, is a threat to the legal system that uses violence for legal ends that the law itself legitimates (such as police or military violence). This indicates the law's "monopoly on violence" as Benjamin puts it, in not simply preserving legal ends but more importantly in preserving the institution of the law itself. It also affirms the threat of actions that are outside of the law, and how even oppositional kinds of action or protests are tolerated when they affirm the power of the law to guarantee certain freedoms.

One important exception is the right to strike, conceded by the state in recognition of the inevitability of antagonism in the workplace. Whether overtly violent or not, the motivation to strikeis to address the violence imposed on the worker by the employer. In this way, and as Trotsky pointed out in his essay "Terrorism" (1911), arguments against the use of violence are inherently hypocritical. In his view, the entire state apparatus and its lawsare an apparatus of terrorism in itself. [6] On the one hand terrorist violence is seen to be inadmissible by the moral order, and yet on the other, in exceptional circumstances it is seen to be necessary according to the self-interest of the state. Much the same paradox applies in contemporary discussions, where in the 'state of emergency' becomes the justification for the erosion of human rights and freedoms. The duplicity is evident in the way those deemed danger to national security can be taken into custody and detained without trial or other sovereign states can be invaded in contravention with international law.

This paradoxical condition has been discussed in depth in Giorgio Agamben's *State of Exception* (2005), extending Carl Schmitt's *Politische Theologie* of 1922 that established the contiguity between sovereignty andthe state of exception. [7] Agamben argues that the state of exception, although described as a provisional measure in exceptional circumstances, has become the working paradigm of modern government. Under this logic, State power uses violence against an identifiable enemy – often preemptively – so that its use of power appears legitimate despite the active contradiction with its own legal and natural laws. When the required ends cannot be guaranteed by the legal system alone, the repressive state apparatus further exercises violence in the name of counter-terrorism or national security.

Software running over networks is regarded as a threat to security in this way too. In *The Exploit* (2007), Alexander Galloway and Eugene Thacker identify how control is distributed relatively autonomously and at

the same time into directed commands, across horizontal and vertical axes. Indeed networks and sovereignty are not incompatible but exceptional –together related as "sovereignty-in-networks". [8]Correspondingly, the recommendation to those developing oppositional tactics is to take advantage of the vulnerabilities in networks by exploiting power differentials that are inherent to the system. This is precisely how software developers and malware (malicious software) developers operate, as they exploit vulnerable operating systems, internet service and security software – as if following Gilles Deleuze in his "Postscript on Control Societies" (1990): "Computer piracy and viruses, for example, will replace strikes and what the nineteenth century called 'sabotage' ('clogging' the machinery)." [9]

Software violence and counter-violence is propagated through such means to exploit known and potential vulnerabilities in the system. Malware is usually installed via worms, trojan horses or backdoors under a common command and control infrastructure. For instance, a program installed by a botnet can violate a system's hard disc and monitor its user's keystrokes to gather private data (such as sensitive financial information, including credit card numbers and passwords for bank or Paypal accounts) and then distribute the retrieved data over the internet back to the computer running the malware (so-called zombie computer). For example, the function names and keywords below are taken from a popular bot with packet sniffing capabilities to capture online credentials and other information. [10]

boolIsSuspiciousVULN(const char *szBuf) – looks for keywords that indicate vulnerable server versions. Examples include:
• "OpenSSL/0.9.6"
• "Serv-U FTP Server"
• "OpenSSH_2"

boolIsSuspiciousHTTP(const char *szBuf) – may attempt to gather HTTPbased authentication credentials and other valuable data. In this samplebot, the keywords appear to target paypal cookies.
• "paypal"
• "PAYPAL"
• "PAYPAL.COM"
• "paypal.com"
• "Set-Cookie:"

There are countless other examples that illustrate how vulnerabilities can be exploited and how botnets can cause severe disruption to targeted sites. A botnet can control a set of 'hijacked' systems to target systems (e.g. a commercial or government website) with information requests in a distributed denial of service (DDoS) attack. The hacktivist tactics of Lizard Squad, Anonymous, or of Lulz Sec, the splinter group of Anonymous who have been "Laughing at your security since 2011!" exemplify such an approach. [11]These loosely associated networks of activists and hactivists have coordinated various DDoS attacks using forums and social media websites, where instructions were disseminated on how to download attack software to bombard websites with data to try to throw them offline. "Operation Payback" (2010)is a good example, in the targeting of sites that had cut ties with WikiLeaks (such as MasterCard, Visa, and PayPal). [12]

If the parallel development of security and liberalism has already been well established (by Foucault), [13]the issue of security today seems almost reducible to the challenge of managing the inherent vulnerability of networked relations. As such, the system, whether online or offline, needs to distinguish whether you are a friend or not, evoking Carl Schmitt's notion of enmity (in *The Concept of the Political*, of 1927). [14] Under contemporaryneo-liberal conditions, it is clear that democracies already exert forms of violence on citizens in subtle ways: the "violence of participation" as Markus Meissen puts it. [15] In other words, democracies exert a form of violence that doesn't appear violent at all such as encouraging the use of certain kinds of social media where friendship is privileged over antagonism. The double standards are agreed to when the user agrees to the terms of service.

In what Angela Mitropoulos has referred to as "softwar" (2007), [16] violence is exerted on users, not least forcing them to pay and upgrade regularly when there are viable free alternatives as in the case of proprietary forms. Mitropoulos refers to the issue of intellectual property and related conflicts over sharing digital content, such as those over P2P file sharing. The perpetrator in this case breaks a number of basic principles inherent to network structures where files can be freely copied and shared, and furthermore legislates to normalise this contrariness. The moral ambiguities of software licenses and duplicities of the law are plain, and at the heart of all terms of service agreements and copyright regimes. To break a contract is to activate the threat of violence enforced by the law, whereas the greater violence has already been committed and gone unpunished in the first place.

When no other choice is possible, software counter-violence might be a justifiable moral if not legal response and there are many other examples of software direct action and hacktivism to further stress this point.(Whistle blowing operates a parallel moral imperative as with the Snowden case, or Wikleaks more broadly.)Hackers are generally understood as those who attempt to penetrate security systems on remote computers, but this is a pejorative use of the term. In general it simply refers to a person who is capable of creating hacks, or demonstrating technical virtuosity. [17]
To clarify the distinction: a hacker is thus someone with proficiency and practical understanding of the structure and operations of computer networks and systems, whereas crackers or system intruders are hackers with malign intentions (more like terrorists if we accept the paradox of that term). The ethical principles of hacking clarifies the distinction:

* Access to computers – and anything that might teach you something about theway the world really works – should be unlimited and total.
Always yield to the Hands-On Imperative!
* All information should be free.
* Mistrust authority – promote decentralization.
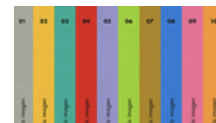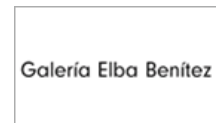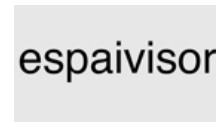* Hackers should be judged by their acting, not bogus criteria such as degrees,age, race, or position.
* You can create art and beauty on a computer.
* Computers can change your life for the better.
* Don't litter other people's data.
* Make public data available, protect private data. [18]

Following these principles, it should be stated that the majority of hackers condemn attacks. The use of *non-violent* direct action and tactical media is more commonplace, such as the FloodNet software developed in 1998 by the Electronic Disturbance Theater, and used by the Zapatistas. [19] For some hackers, the ethical practices of free software represent a move away from the use of overt violence but the paradoxes of power simply cannot be avoided. It is this issue that this essay tries to establish: how violence is inherent to software. Perhaps more contemporary examples of online violence serve to emphasise how software itself contains active contradictions that oscillate between truth and falsity (like Boolean logic or negative dialectics), between violence and non-violence.

Lizard Squad's DDoSattack on the free software Tor browsing network in January 2015 makes a case in point (Tor prevents others from learning your location or browsing habits). [20] The attack aimed to highlight vulnerabilities with respect to Tor's ability to enable anonymity on the Internet and thereby to remain outside the reach of government monitoring agencies like the NSA. By attacking nodes used to relay information between peers, and setting up new relays called "LizardNSA", Lizard Squad could begin to piece together communications that were transmitted under the belief that the information was anonymous. The action enraged other hacker groups such as Anonymous who released the following Twitter message: "Hey @LizardMafia don't f—k with the Tor network. People need that service because of corrupt governments. Stand the f—k down." [21]

The questionable ethics of the action in response to debates about Internet freedom operates in a similar way to the paradoxes of free software and free speech as if it were not already a problematic concept. [22] The ethics of free software emerged out of the hacker communities yet the ambiguities of free speech as the central analogy have not been critically developed inasmuch as it is enshrined in the liberal tradition that recognizes that suppressing freedom of speech is a crude tactic of governance. Instead the state, for the most part, opens up the widest possible domains for the expression of opinions that become constituent of its own exercise of power protected under international law.

The Universal Declaration of Human Rights states that: "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." [23] Article10 of the European Convention on Human Rights similarly provides the right to freedom of expression, but like Article 19 is also subject to certain restrictions that are deemed "necessary in a democratic society." [24] This allows restrictions for the interests of national security, or public order, or protection of public health and morals, and soon. It leaves freedom on the Internet, as with life in general, subject to both state and market regulation, and further compromised by the pervasive use of filtering software and data veillance practices. Therefore it arguably becomes necessary to produce paradoxes at the level of software in recognition of its central role in the structural logic of capitalism. The violence embodied in software is inherent to the way it prescribes and determines certain actions. Like the myth of freedom of choice, violence is demonstrated at multiple levels of execution, and exerted against information hat wants to be free.

In Benjamin's "Critique of Violence", he describes the potential for 'pure immediate violence" – human action that neither makes nor preserves law, but is outside of the law altogether. [25] The idea of pure violence does not apply to any violent action in itself, but in its relation to the conditions under which it is constituted. The concept draws together class violence with the theology of divine violence represented by Judaic Messianism- where redemption is provided by pure divine violence. So rather than promoteterrorist violence, he instead calls for "collective political action that is lethal not to human beings, but to the humanly created mythic powers that reign over them". [26] The concept of pure violence is a violence that appears to come from nowhere – from beyond the law – in which "killing is neither a crime nor a sacrifice" according to Žižek, because law applies only to the living: "Divine violence isan expression of pure drive, of the undeadness, the excess of life, which strikes the "bare life" regulated by law." [27] This is an action that lies in excess of violence and terrorism, or the shootings in Paris or Copenhagen, [28] and more in the realm of the nonhuman. One might speculate that software might similarly express pure means through the use of distributed software, if directed at the sovereign technical infrastructures that already exert forms of violence. If no one will protect us from the violence inflicted upon us by software, there is no choice but to engage the mythic powers that regulate our operating systems at the level of software itself.

[1] For more on botnets, and links to other technical terminology, see http://en.wikipedia.org/wiki/Botnet.

[2] Judith Butler, *Excitable Speech: A Politics of the Performative*, London: Routledge 1997, 1; she is referring to Althusser's notion of interpellation. Also see Geoff Cox & Alex McLean, *Speaking Code: Coding as Aesthetic and Political Expression*, Cambridge, Mass.: MIT Press, 2013.

[3] SlavojŽižek,*Violence: Six Sideways Reflections*, London: Picador, 2008, 52 & 58.

[4] Walter Benjamin (1996 [1921]) "Critique of Violence", in Marcus Bullock & Michael W. Jennings, eds. *Walter Benjamin: Selected Writings, Volume 1, 1913-1926*, Cambridge, Mass.: Harvard University Press, pp. 236-252. In addition, the question of violence is addressed by many others, such as: Hannah Arendt's "On Violence" (1969); Pierre Clastres's "Archaeology of Violence" (1979); Frantz Fanon's *The Wretched of the Earth* (published in French as *Les damnés de la terre*, 1961) in which violence opposes the violence of colonialism; Georges Sorel's "Reflections on Violence" (1915); and Irving Wohlfarth's "Critique of Violence" (2009) which charts the connections between Benjamin's essay and the Red Army Faction operating in Germany during the 1970s.

[5] Benjamin, "Critique of Violence", 236 & 237.

[6] Leon Trotsky (1987 [1911]) "Terrorism", in *What do we mean…?,Education for Socialists*: No. 6, March, London Socialist Worker's Party; available at http://www.marxists.de/theory/whatis/terror2.htm

[7] Giorgio Agamben, *State of Exception*, Chicago: University of Chicago Press, 2005.

[8] Alexander R. Galloway and Eugene Thacker, *The Exploit: A Theory of Networks*, Electronic Mediations,

Vol. 21, Minneapolis: University of Minnesota Press, 2007.

[9] Gilles Deleuze, "Postscript on the Societies of Control", in *October*, Vol. 59 (Winter, 1992), 3-7.

[10] Examples from Nicholas Ianelli& Aaron Hackworth "Botnets as a Vehicle for Online Crime", CERT Coordination Center, Carnegie Mellon University, 2005; available at http://www.cert.org/archive /pdf/Botnets.pdf.

[11] See Gabriella Coleman, *Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous*, London: Verso, 2014.

[12] See http://en.wikipedia.org/wiki/Operation_Payback

[13] See Giorgio Agamben, "On Security and Terror", in Geoff Cox & Wolfgang Sützl, eds.,*Creating Insecurity: Art and Culture in the Age of Security*, New York: Autonomedia, 2009, 23-25. The original version appeared in *Frankfurter AllgemeineZeitung*, Sept 20, 2001, in German.

[14] Carl Schmitt, *The Concept of the Political*, Chicago: University of Chicago Press, 1996 [1927]. Schmitt's critique of liberalism lies in its inability to recognizeor enemy is at the centre of this. But, as liberal democracies are seen to be inadequate, the consequence of this for Schmitt was a legitimation of authoritarian regimes.

[15] Markus Miessen, ed. *The Violence of Participation*, Berlin: Sternberg Press, 2007, 26. See also Clare Bishop, *Artificial Hells: Participatory Art and the Politics of Spectatorship*. London: Verso, 2012.

[16] Angela Mitropoulos, "The Social Softwar", in *Web 2.0: Man's Best Friendster?,Mute,* Vol. 2 (4), January 2007; available at http://www.metamute.org/Web-2.0-Mans-best-friendster/.

[17] Steven Levy, *Hackers: Heroes of the Computer Revolution*, Project Gutenberg Etext, 1984; available at http://www.ibiblio.org/pub/docs/books/gutenberg/etext96/hckrs10.txt.

[18] "Hacker Ethics", http://www.ccc.de/hackerethics?language=en.

[19] The Electronic Disturbance Theater (EDT) initially executed FloodNet in April and December 1998 on Mexican and American government sites respectively. FloodNet can also be downloaded from the site (http://www.thing.net/~rdom/ecd/floodnet.html). For more on the Zapatistas, see their official site (http://www.ezln.org.mx/index.html) and Wikipedia entry that includes a section on the use of tactical media (http://en.wikipedia.org/wiki/Zapatista_Army_of_National_Liberation). Also see Brett Stalbaum, "The Zapatista Tactical FloodNet: A collaborative, activist and conceptual art work of the net" (2002); available at http://www.thing.net/~rdom/ecd/ZapTact.html.

[20] Tor Project, https://www.torproject.org/.

[21] Quinten Plummer, "Tor Attack Pits Anonymous Against Lizard Squad: PSN and Xbox Live Back Online", *Tech Times*, 01 Jan 2015, http://www.techtimes.com/articles/23334/20150101/tor-attack-pits-anonymous-against-lizard-squad-psn-and-xbox-live-recovering.htm

[22] To be clear, I am referring to how the Free Software Foundation define freedom: "'Free software' is a matter of liberty, not price. To understand the concept, you should think of 'free' as in 'free speech', not as in free beer." Available at https://www.gnu.org/philosophy/free-sw.html.

[23] The Universal Declaration of Human Rights (adopted in 1948); available at http://www.un.org /en/documents/udhr/.

[24] The European Convention on Human Rights (adopted in 1950); available at http://www.hri.org /docs/ECHR50.html.

[25] Discussion of Benjamin's essay and its rejection of the law for "messianic anarchy" appears in Irving Wohlfarth's "Critique of Violence: the deposing of the law", in *Radical Philosophy*, Jan/Feb: 153 (2009), 13-26.

[26] Susan Buck-Morss, *Thinking Past Terror: Islamism and Critical Theory on the Left*, London: Verso, 2003, 33.

[27] Žižek, Violence, 168.

[28] I refer to two events at the beginning of 2015: the Charlie Hebdo shootings in Paris (7 Jan) provoked by satiric images of Mohammad and their earlier re-publication of the *Jyllands-Posten* cartoons of Muhammad in 2006; and the shootings at the public event "Art, Blasphemy and Freedom of Expression" at the Krudttønden cultural centre, Copenhagen (14-15 Feb), where Swedish artist Lars Vilks was in attendance and thought to have been the main target because of his drawings of Muhammad.