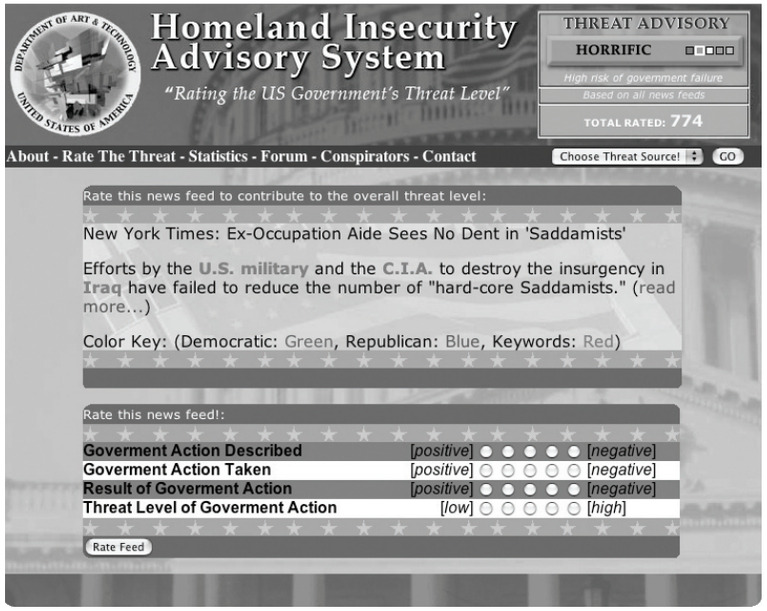
CRITIQUE OF SOFTWARE SECURITY

Geoff Cox & Martin Knahl



Screenshot: Jonah Brucker-Cohen, Michael Bennett, Homeland Insecurity Advisory System (2004)

Security is predicated on protection from perceived violence or terrorism, but who will protect us from security? Behind this statement is the fact that those in power regularly commit acts of real and symbolic violence and this goes unpunished – indeed it is legitimated so effectively that we think we are protected by these acts of violence against us in the form of security. This essay asks how the inherent violence encoded into software might be understood in this way. The arguement is that – rather than simply assuming that it protects the user from insecurity - security software itself constitutes violence. These are some of the conditions that produce states of emergency and that in turn create insecurities.

Critique of Violence

The background to this line of thinking draws upon Walter Benjamin's 1921 essay 'Critique of Violence'.[1] For Benjamin, the issue is not whether violence is a means to a just or unjust end (a critique of 'just ends') 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' (1996: 236).[2] Rather than simply reconciling just ends by a justification of the means, or vice versa, the 'Critique of Violence' essay focuses on the realm of means, or more precisely: 'the question of the justification of certain means that constitute violence' as Benjamin puts it (1996: 237).

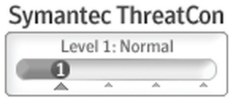
As far as the State is concerned, violence exercised by individuals, or its legal subjects, is a threat to the legal system that serves to justify its own use of violence. Legal ends appear to be only achievable by legal power. The law uses violence for legal ends that the law itself has decided. For instance, and as an agent of State authority, police violence is legitimated as both law-making and law-preserving – and indeed *all* violence is a means of law-making and law-preserving according to Benjamin. This indicates the law's 'monopoly on violence' as he puts it, in not simply preserving legal ends but more importantly in preserving the law itself. It also affirms the threat of actions that are outside of the law, to the law itself, and why they must be contained.

An exception to this is the right to strike, conceded by the State in recognition of the inevitability of antagonism in human societies. Yet to strike is an active refusal to work, the withdrawal of actions, a non-action, and is not necessarily violent. Where violence is more easily discernible is that the motivation to strike in the first place is to escape from the violence imposed on the worker by the employer. This position is in keeping with Trotsky, in his essay 'Terrorism' of 1911, who considers arguments against the use of violence to be a hypocrisy in that the entire state apparatus and its laws, police, and army are nothing but an apparatus for capitalist terror:

'Our class enemies are in the habit of complaining about our terrorism. What they mean by this is rather unclear. They would like to label all the activities of the proletariat directed against the class enemy's interests as terrorism. The strike, in their eyes, is the principal method of terrorism. The threat of a strike, the organisation of strike pickets, an economic boycott of a slave driving boss, a moral boycott of a traitor from our ranks - all this and much more they call terrorism. If terrorism is understood in this way as any action inspiring fear in, or doing harm to, the enemy - then of course the entire class struggle is nothing but terrorism.' (1987)

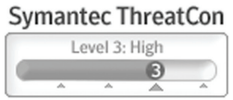
The right to strike translates as the right to use a form of violence to attain certain ends, and the State reserves the right to counter this with violence.[3] Trotsky points to the glaring paradox of a value system that argues for the 'absolute value of human life' and at the same time sacrifices millions of people in wars. On the one hand violence is seen to be inadmissible, and yet on the other, in *exceptional circumstances* it is seen to be necessary – in a 'shift from the moral high ground to raw self-interest' (Buck-Morss 2003: 33).[4]

Much the same paradox applies in the contemporary 'war on terror', as the *state of emergency* becomes the justification for the erosion of citizen's rights and freedoms that were hard won. The duplicity is evident in the way those deemed a danger to national security can be taken into custody and detained in ways



ThreatCon Level 1
Low : Basic network posture
This condition applies when there is no discernible network incident activity and no malicious code activity with a moderate or severe risk rating. Under these conditions, only a routine security posture, designed to defeat normal network threats, is warranted. Automated systems and alerting mechanisms should be used.

ThreatCon Level 2
Medium : Increased alertness
This condition applies when knowledge or the expectation of attack activity is present, without specific events occurring or when malicious code reaches a moderate risk rating. Under this condition, a careful examination of vulnerable and exposed systems is appropriate, security applications should be updated with new signatures and/or rules as soon as they become available and careful monitoring of logs is recommended. Changes to the security infrastructure are not required.



ThreatCon Level 3
High : Known threat
This condition applies when an isolated threat to the computing infrastructure is currently underway or when malicious code reaches a severe risk rating. Under this condition, increased monitoring is necessary, security applications should be updated with new signatures and/or rules as soon as they become available and redeployment and reconfiguration of security systems is recommended. People should be able to maintain this posture for a few weeks at a time, as threats come and go.

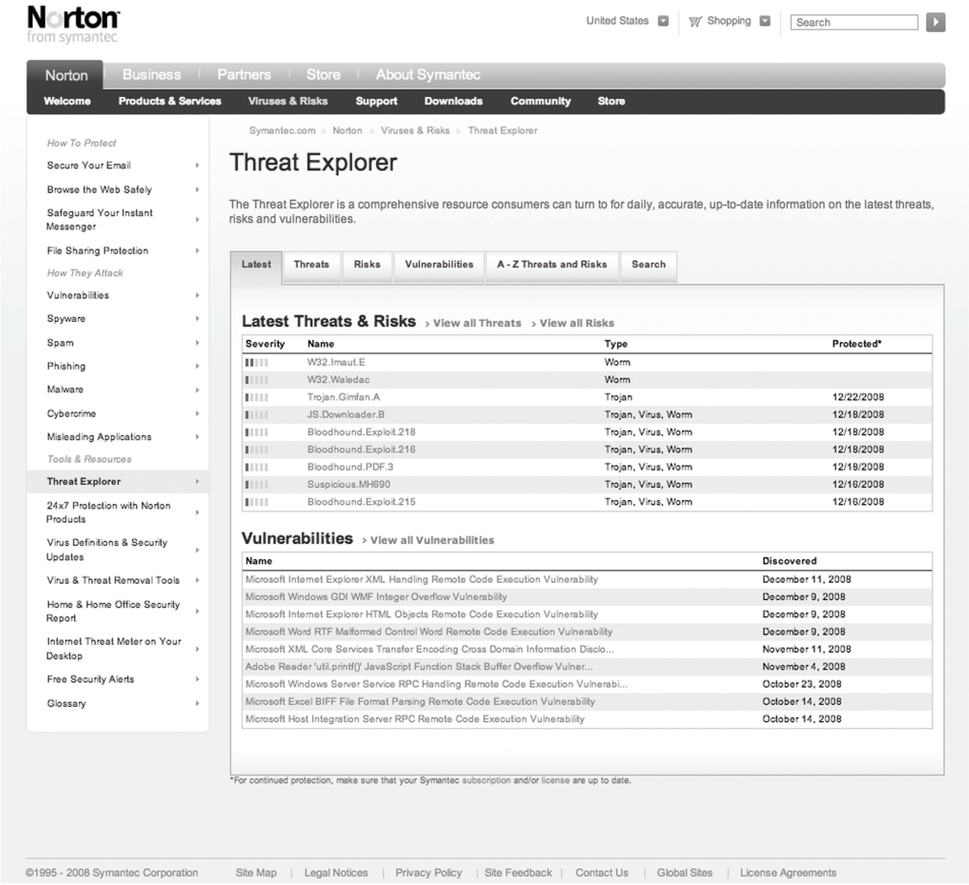
ThreatCon Level 4
Extreme : Full alert
This condition applies when extreme global network incident activity is in progress. Implementation of measures in this Threat Condition for more than a short period probably will create hardship and affect the normal operations of network infrastructure.

that erase individual human rights, turning them into a 'noncitizen' such that 'bare life reaches its maximum indeterminacy' (Agamben 2005: 4). The way the State suspends and withdraws its guarantee of protection and legal entitlement is a condition of contemporary power, and this is 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 and the state of exception, Agamben argues that the state of exception, although described as a provisional measure in *exceptional circumstances*, has become the working paradigm of modern government.[5] Under this logic, State power uses violence against an identifiable enemy 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 intervenes 'for security reasons' (Benjamin 1996: 243). Security marks the exception, in other words.

Software Violence

Software running over networks is a manifestation of ideology, and connectivity remains a security threat beyond its purely technical functionality. This is what Alexander Galloway and Eugene Thacker, in *The Exploit*, describe as the new 'network-network symmetry' of power, in which control is distributed relatively autonomously in horizontal organisational locales and at the same time into rigid vertical hierarchies or directed commands (2007). This description is a socio-technical truism of course, and one that supports their claim that networks and sovereignty are not incompatible. Indeed together they are *exceptional* and are always related as 'sovereignty-in-networks'. Correspondingly, the recommendation to those developing oppositional tactics is to take advantage of the vulnerabilities in networks by exploiting power differentials that exist in the system. This is precisely what software developers and malware (malicious software) authors have discovered, as they exploit vulnerable operating systems, internet service and security software.

To add detail here: Internet violence is propagated through various means such



images: Symantec <http://www.symantec.com/>

as the use of viruses, spam, click fraud, phishing, and 'botnets' (collections of software robots, or bots, that run autonomously).[6] A vast amount of terms such as these has evolved in the area of software security,[7] and more or less structured collections exist either in the form of security-industry recommendations (see Symantec images) or as standards for research. An understanding of the characteristics and nature of known vulnerabilities has also been organised into taxonomies, providing a framework for the examination of known and potential

future vulnerabilities (Igure & Williams 2008).[8] Malware is usually installed via worms, trojan horses or backdoors under a common command and control infrastructure. 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 to its 'master'. 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 (from Ianelli & Hackworth 2005):

```
bool IsSuspiciousBot(const char *szBuf) — looks for keywords related to
bot activity. Some examples include:
· "JOIN #"
· "302 "
· "366 "
· ":.login"
· ":!login"
· ":!Login"
· ":.Login"
· ":.ident"
· ":!ident"
· ":.hashin"
· ":!hashin"
· ":.secure"
· ":!secure"

bool IsSuspiciousIRC(const char *szBuf) — looks for keywords related to
interesting IRC activity. Examples include:
· "OPER "
· "NICK "
· "oper "
· "You are now an IRC Operator"

bool IsSuspiciousFTP(const char *szBuf) — looks for FTP authentication
credentials triggered by keywords such as USER and PASS.

bool IsSuspiciousHTTP(const char *szBuf) — may attempt to gather HTTP
based authentication credentials and other valuable data. In this sample
bot, the keywords appear to target paypal cookies.
· "paypal"
· "PAYPAL"
· "PAYPAL.COM"
· "paypal.com"
· "Set-Cookie:"

bool IsSuspiciousVULN(const char *szBuf) — looks for keywords that
indicate vulnerable server versions. Examples include:
· "OpenSSL/0.9.6"
· "Serv-U FTP Server"
· "OpenSSH_2"
```

There are countless other cases that illustrate insecurity issues surrounding botnets and the ways in which vulnerability in the system is exploited. With the popularity of filesharing and the high volumes of computers connected to peer to peer (P2P) networks, they have also become increasingly open to attack. The Trojan.Peacomm is an example of a trojan horse that provides the basis for building a P2P botnet (Grizzard 2007). The threat typically arrives in an email with a subject (e.g. 'U.S. Secretary of State Condoleezza Rice has kicked German Chancellor Angela Merkel'), and attachments (e.g. 'Full Story.exe') and an empty body. The executable is a trojan horse which modifies a system's services .exe process and adds hidden threads. The 'infected' system subsequently attempts to establish P2P communication via UDP using a set of given IP addresses to obtain additional malicious files. Using a firewall with egress filtering, it can be detected that the services.exe process attempts to connect to a remote address via a UDP port. Subsequently the system will receive additional IP addresses, in essence building up a distributed network. To facilitate the process, the trojan further maintains a list of unsuitable peers. The strategy of using P2P communication spreads the load and further improves the robustness of the botnet, particularly when compared to the traditional approach of using centralised command and control servers.[9]

Botnets can also cause severe disruption on 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. In the extreme, a system that is unable to handle excessive crashes, sometimes brings down an entire data centre with it. In May 2006, the American blog-publishing firm Six Apart found itself the victim of a DDoS assault by an especially aggressive botnet. Within minutes, the company's servers had crashed, causing the blogs of 10 million customers to disappear. Six Apart eventually discovered that the attack was not aimed at itself but rather at one of its customers, an Israeli firm named Blue Security, which had caused ignominy by offering a spam-counter attack service (Berinato 2006).[10] However the botnet assault continued for weeks, damaging many other companies and sites.

Eventually Blue Security surrendered and went out of business, expressing their reluctance (unlike the Israeli State) to take part in an ever-escalating 'soft war' of violence and counter-violence. The point is that security software operates double standards.

It would seem that the issue of security is reducible to the challenge of managing the inherent insecurities of networked relations. In other words, the network 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).[11] Under contemporary neo-liberal conditions – inextricably linked to security – it is clear that liberal democracies exert a form of violence through their insistence on friendliness and participation in networks. This is the organised violence of democracy or 'violence of participation', as Markus Meissen puts it (2007: 26).[12] In other words, liberal democracy exerts a form of friendly violence that doesn't appear violent at all – such as encouraging the use of certain kinds of software. All the time the violence is exerted nonviolently under the guise of protection from violence: security.

Software Nonviolence

When no other choice is possible, software violence might be the answer – replacing the strike in the form of software that Deleuze anticipated when he claimed: 'Computer piracy and viruses, for example, will replace strikes and what the nineteenth century called "sabotage" ("clogging" the machinery).' (1990) There are many examples of artists and activists working in this way through direct action and hacking. Hackers, crackers,[13] or system intruders 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 was capable of creating hacks, or demonstrating technical virtuosity (Levy 1984). The ethical principles of hacking reflect these concerns:

'* Access to computers – and anything that might teach you something about the way 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.'[14]

In keeping with these principles, it should be stated that most hackers condemn attacks against communication systems. In 1999, the Chaos Computer Club joined an international coalition of hacker groups (including the Cult of the Dead Cow)[15] to condemn the use of networks as battlegrounds in their declaration for 'info peace': 'DO NOT support any acts of "Cyberwar". Keep the networks of communication alive. They are the nervous system for human progress.'[16]

An excellent example of non-violent direct action is the FloodNet tactical software developed in 1998 by the Electronic Disturbance Theater.[17] The FloodNet implementation is based on Java applets that assists in the execution of virtual sit-ins or online civil acts of disobedience, and offered as a tool to enable protestors to effectively shut down web servers of target institutions, by flooding them with requests. The requests are automatically reloaded at high frequencies to cause an excessive amount of traffic on the server so that other users are not able to access the website. It further enables users to post statements to a targeted site by transmitting them to the server's log files:

'By the selection of phases for use in building the "bad" urls , for example using "human_rights" to form the url "http://www.xxx.gb.mx/human_rights", the FloodNet is able to upload messages to server error logs by intentionally asking for a non-existent url. This causes the server to return messages like "human_ rights not found on this server." This works because of the way many http servers

process requests for web pages that do not exist. FloodNet's Java applet asks the targeted server for a directory called, in this example, "human_rights", but since that directory doesn't exist, the server returns the familiar "File not Found" or "Error 404" message, recording the bad request. This is a unique way to leave a message on that server.' (Stalbaum)[18]

The tactic follows the hacker sensibility in opening up existing security vulnerabilities in the system. As ever, power continues to produce its own vulnerability but the question of violence is more unsettling and paradoxical. For some hackers, the ethical practices of free software represent a move away from the use of violence.[19] However what this essay has tried to establish is how violence is simply unavoidable and is inherent to the socio-technical structures of networks. In addition, insecurity is promoted by a burgeoning security industry that creates both awareness and fear regarding perceived insecurity,[20] intensifying the dependency of users on its software and at the same time engendering a growing ambivalence even amongst security professionals who recognise that 'security causes its own type of harm'.[21]

The actions of software dissidents can be seen to extend network forms of antagonism and the justification of certain means that constitute violence – further evoking Benjamin's essay. Moreover, software is necessarily violent even when it appears nonviolent.

Pure Software Violence

In addition to 'systemic violence', there is symbolic violence embodied in language itself - not simply as an incitement to a violent action or in the ways that language reflects social domination (e.g. 'man-made' language) or heavy critique in general – but in the way that it produces meaning more fundamentally. For instance, in saying that 'a fundamental violence exists in this "essencing" ability of language' (2008: 58), Slavoj Žižek is making reference to Hegel's observation that there is something inherently violent in the capacity of language to represent a thing – an act equivalent to its symbolic death. In the realm of software,

programming languages are even more overtly violent – not simply representing a thing but enacting it. In other words, if source code says something and does something at the same time, it symbolises *and enacts* violence on the thing. It literally *executes it*.

In writing these words on a computer, violence and counter-violence is demonstrated in the choice of software and operating systems. Software development is limited through force. Violence is exerted against information that wants to be free. In what Angela Mitropoulos refers to as the 'softwar' (2007) proprietary software commits violence against users, all the time forcing users to pay and upgrade regularly when there are viable free alternatives. Mitropoulos is more specifically referring 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 digital media processes where files can be freely copied and shared, and furthermore legislates to normalise this contrary way of working. The moral ambiguities of software licenses and duplicities of the law are clear, and at the heart of all contractual agreements. 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. This is the basis for the piracy ethic, in stealing back what was already stolen in the first place.

On the relation between violence and social transformation, Benjamin refers to Georges Sorel's essay 'Reflections on Violence' (1915) to expose the distinction between violence and force (1996: 245-6).[22] Sorel points to the failure of parliamentary democracy to deliver its promises and to the principle of counter-violence, not only through strikes but through revolution. The point is that under certain conditions violence becomes force, as 'pure means'.[23] The consequences of the disruption of means and ends are political, as Agamben confirms: 'Politics is the sphere neither of an end in itself nor of means subordinated to an end; rather, it is the sphere of a pure mediality without end intended as the field of

human action and of human thought.' (2000: 116)

In Benjamin's 'Critique of Violence', the concept of pure means invokes the potential for 'pure immediate violence' – human action that neither makes nor preserves law, but is outside of the law. The idea of 'pure violence' does not apply to any violent action in itself, but in its relation to external conditions. The present is seized from the impure violence of history in what Benjamin describes as the 'real state of emergency' (Wohlfarth 2009: 14).[24] The paradox of Benjamin's position is in drawing together proletarian violence (informed by Marxism) with the theology of divine violence represented by Judaic Messianism - where redemption is provided by 'pure divine violence'. So rather than promote terrorist violence, or as necessary means justified by ends, he calls for: 'collective political action that is lethal not to human beings, but to the humanly created mythic powers that reign over them' (Buck-Morss 2003: 33). The concept of pure, divine 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. Žižek continues: 'Divine violence is an expression of pure drive, of the undeadness, the excess of life, which strikes the "bare life" regulated by law.' (2008: 168). For Benjamin, revolution requires this sense of excess; or in Agamben's words, it is a means without end.

With software, pure means opens up vulnerabilities in the system as a practice of creating insecurity. If no one will protect us from the violence of security, there is no option but to release 'pure softwar' – as resistance to the mythic powers that regulate our systems.

↻

NOTES:

1. In addition to Benjamin, it should be said that the question of violence is addressed by many others, such as those mentioned in the text, but also: Hannah Arendt's 'On Violence' (1969), Pierre Clastres's 'Archaeology of Violence' (1979), and 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. In attempting to actualise the 'Critique of Violence', the excesses of the Red Army Faction operating in Germany during the 1970s are often cited. Irving Wohlfarth's 'Critique of Violence' (2009) charts the connections/disconnections between Benjamin's 'Critique' and the RAF's violent interpretation.

2. This is important to Benjamin's argument as otherwise violence operates as if by 'natural law', in a Darwinian fashion as 'the only original means, besides natural selection, appropriate to all the vital ends of nature' (1996: 237). In contrast to natural law that takes violence to be a product of nature, 'positive law' takes violence as a product of history. The problem is that 'positive law is blind to the absoluteness of ends, natural law is equally so to the contingency of means' (1996: 237). Whereas natural law seeks to justify means, positive law tries to guarantee ends.

3. What is distinguished in Trotsky's formulation is not individual terrorist acts, but collective acts against the system. He says: 'In our eyes, individual terror is inadmissible precisely because it *belittles the role of the masses in their own consciousness*, reconciles them to their powerlessness...' (1987). Moreover, Capitalist society allows strikes on the basis that it requires an active, mobile, cognitive, communicative and socialised labour force, but it is the self-recognition of this, that is necessary in Trotsky's view to consolidate self-organisation that leads to the strategic 'alignment of class forces, the proletariat's social weight'.

4. Susan Buck-Morss points to the flagrant opportunism of the US in this respect, and the West in general, in how it approaches 'democracy' with double standards. She quotes Samuel Huntington: 'Democracy is promoted but not if it brings Islamic fundamentalism to power; nonproliferation is preached for Iran and Iraq but not for Israel... human rights are an issue with China but not with Saudi Arabia' (2003: 32). The present terrorism of Israeli actions in Gaza confirms the point all too clearly (January 2009). Furthermore, IAA's *Terminal Air* project (herein) is another example of double standards or what they call 'implausible deniability'.

5. That security is the leading principle of state politics is also emphasised in Agamben's 'On Security and Terror' (herein), such that the State 'can always be provoked by terrorism to become itself terrorist' (2001).

6. The term botnet refers to a network of computers using distributed computing software but is typically associated with compromised computers (sometimes also referred to as Zombie computers) running malicious software. For more on botnets, and links to other technical terminology, see the wikipedia entry <http://en.wikipedia.org/wiki/Botnet>.
Some computer security experts believe that at least 10% of home PCs have been recruited into botnets (Carr 2007). The majority of these computers are running Microsoft Windows operating systems, but other operating systems can be affected.

7. Examples include: 'the most trusted source for computer security training, certification and research' <http://www.sans.org/resources/glossary.php>, '... 10 biggest network threats' <http://www.itsecurity.com/features/networksecurity-threats-011707/>, Internet Engineering Task Force IETF RFC4949 <http://www.rfc-editor.org/rfc/rfc4949.txt> and RFC2828 that provide extensive Internet Security Glossaries (e.g. RFC4949 totals 365 pages).

8. Vinay M. Igure and Ronald D. Williams (2008) suggest the following properties for an efficient taxonomy of attacks and vulnerabilities in Computer Systems: Application — or system-specific taxonomy; Taxonomy must be layered or hierarchical; First level of classification — attack

impact; Second level of classification — system-specific attack; Third level of classification — system components (attack targets); Fourth level of classification — system features (source of vulnerability); Classes need not be mutually exclusive.

9. A useful project in relation to this rise in the abuse of P2P networks is 'Six/Four', 'a flexible framework consisting of a formally specified P2P protocol. This protocol is best described as a trust-enhanced anonymous tunneling protocol, and meant to provide people with anonymous, secure access to public data.' <http://www.hacktivismo.com/projects/index.php> Download from <http://sourceforge.net/projects/sixfour/>.

10. Blue Security's URL <http://bluesecurity.com/> is now a dead link. For a description of the anti-spanning tool and subsequent backlash, see <http://en.wikipedia.org/wiki/Blue_Frog>.

11. Schmitt's critique of liberalism lies in its inability to recognise antagonism as inevitable in human societies, and the political differentiation of friend or enemy lies at the centre of this. But, as liberal democracies are seen to be inadequate, the consequence of this for Schmitt is a legitimation of authoritarian regimes.

12. Social networking platforms arguably demonstrate the 'violence of participation'. For more on this, see *Antisocial Applications* <http://project.arnolfini.org.uk/projects/2008/antisocial/notes.php>.

13. To clarify the distinction: a hacker is thus someone with proficiency and practical understanding of the structure and operations of computer networks and systems. Those with more malign intentions are sometimes known as crackers (aka terrorists).

14. From 'Hacker Ethics' <http://www.ccc.de/hackerethics?language=en>. Also see Steven Mizrach's 'Is there a Hacker Ethic for 90s Hackers?', http://www.fiu.edu/~mizrachs/hackethic.html

15. The Cult of the Dead Cow (cDc) is an extremely influential hackers group, established in 1984, and opposing anyone or any government that aspires to limit free speech <http://www.cultdeadcow.com>. For instance, its global campaign against Google was launched in 2006, and Goolag Scanner was released in 2008 <http://www.goolag.org/>.

16. The 1999 declaration of 'info peace' <http://www.ccc.de/CRD/CRD19990107.html> (although this a broken link on the CCC web site). In the wake of 9/11, a Chaos Computer Club press release (of 09/13/2001) further emphasised the point that more international understanding was required not conflict <http://www.ccc.de/press/releases/2001/CCC20010913.en.html>.

17. The Electronic Disturbance Theater (EDT) is a small group of cyber activists and artists engaged in developing the theory and practice of Electronic Civil Disobedience (ECD). The group initially executed FloodNet in April and December 1998 on Mexican and American government sites respectively. The ECD web site <http://www.thing.net/~rdom/ecd/ecd.html> contains a log of current and past actions. FloodNet can also be downloaded from the site <http://www.thing.net/~rdom/ecd/floodnet.html>.

18. The quote continues: 'Past versions of the FloodNet have tuned this idea to current events, such as during the June 10 protest when the names of the Zapatista farmers killed by the Mexican Army in military attacks on the autonomous village of El Bosque, were used in the construction of the "bad" urls. In an artistic sense, this is a way of remembering and honoring those who gave their lives in defense of their freedom. In a conceptual sense, the FloodNet performance was able to facilitate a symbolic return of the dead to the servers of those responsible for their murders.' (op cit.)
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>.

19. Thanks to Jaromil for clarification of this point (from an email exchange in December 2008), and for pointing to the 'info-peace' declaration (see note 16).

20. According to different market surveys the size of the security software market is experiencing rapid growth, fuelled by 'compliance, data leakage and privacy issues, along with the need to tackle the fast evolving and sophisticated threat environment' (Thomson 2008). According to latest figures from Gartner, sales of enterprise security products rose by nearly 20 per cent in 2007 and were worth $10.4bn. Symantec dominates the enterprise security market with over 26 per cent market share, followed by McAfee with over 11 per cent (Thomson 2008).

21. Gerald V Post and Albert Kagan raise the question whether IT controls are a burden or benefit. According to the results of their study: '34% of the respondents perceived interference or delays caused by the security systems as a consequence of their business environment... general employees perceive that increases (more onerous measures) in security policies and practices result in greater interference(s) with their job responsibilities'. Post and Kagan further suggest that users should be part of creating a security policy and suggest the testing of security restrictions on users to minimise task interference.

22. Note the German word 'Gewalt' means both violence and force.

23. The use of the phrase 'pure means' is interesting in this connection as it evokes interlinking ideas expressed in Hannah Arendt's essay 'Labor, Work, Action' (2000) and Giorgio Agamben's short collection of essays *Means Without End* (2000); both making reference to Aristotle's claim that action is an end in itself.

24. An extensive discussion of Benjamin's essay and its reception in relation to a rejection of the law for 'messianic anarchy' appears in Wohlfarth's 'Critique of Violence' (2009). Wohlfarth maintains that the emphasis of politics over history is crucial to a reading of Benjamin's 'Critique', in 'seizing the present'; what Benjamin describes elsewhere as exploding the historical continuum.

REFERENCES:

Giorgio Agamben (2000 [1992]) *Means Without End: Notes on Politics*, trans. Vincenzo Binetti & Cesare Casarino, Minneapolis: University of Minnesota Press.

Giorgio Agamben (2001) 'On Security and Terror', trans. Soenke Zehle, in *Frankfurter Allgemeine Zeitung*, Sept 20 <http://www.egs.edu/faculty/agamben/agamben-on-security-and-terror.html>.

Giorgio Agamben (2005) *State of Exception*, trans. Kevin Attell, Chicago: University of Chicago Press.

Hannah Arendt (2000 [1964]) 'Labor, Work, Action', in *The Portable Hannah Arendt*, New York: Penguin, pp. 167-181.

Paul Barford & Vinod Yegneswaran (2006) 'An Inside Look at Botnets', *Advances in Information Security*, Springer <http://pages.cs.wisc.edu/~pb/botnets_final.pdf>.

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.

Scott Berinato (2006) 'Attack of the Bots', *Wired*, Issue 14 (11), November.

Konstantin Beznosova & Olga Beznosova (2007) 'On the imbalance of the security problem space and its expected consequences', *Information Management & Computer Security*, Vol. 15 (5), Emerald Group Publishing Limited, pp. 420 – 431.

Susan Buck-Morss (2003) *Thinking Past Terror: Islamism and Critical Theory on the Left*, London: Verso.

Nick Carr (2007) 'Botnets - a hidden menace that threaten the future of the internet', *The Guardian*, 5 April.

Gilles Deleuze (1990) 'Control and Becoming', conversation with Antonio Negri, in *Futur Anterieur*, trans. Martin Joughin <http://www.generation-online.org/p/fpdeleuze3.htm>

Alexander R. Galloway & Eugene Thacker (2007) *The Exploit: A Theory of Networks*, Electronic Mediations, Vol. 21, Minneapolis: University of Minnesota Press.

Julian Grizzard et al (2007) 'Peer-to-Peer Botnets: Overview and Case Study', *HotBots '07*, 4th USENIX Symposium on Networked Systems Design & Implementation, Cambridge (MA), 11-13 April.

Nicholas Ianelli & Aaron Hackworth (2005) 'Botnets as a Vehicle for Online Crime', CERT Coordination Center, Carnegie Mellon University <http://www.cert.org/archive/pdf/Botnets.pdf>.

Vinay M. Igure & Ronald D. Williams (2008) 'Taxonomies of Attacks and Vulnerabilities in Computer Systems', in *IEEE Communications Surveys & Tutorials*, 1st Quarter: Vol. 10 (1) <http://www.comsoc.org/pubs/surveys>.

Steven Levy (1984) *Hackers, Heroes of the Computer Revolution*, *Project Gutenberg Etext of Hackers* <http://www.ibiblio.org/pub/docs/books/gutenberg/etext96/hckrs10.txt>.

Markus Miessen, ed. (2007) *The Violence of Participation*, Berlin: Sternberg Press.

Angela Mitropoulos (2007) 'The Social Softwar', in *Web 2.0: Man's Best Friendster?*, *Mute*, Vol. 2 (4), January <http://www.metamute.org/Web-2.0-Mans-best-friendster/>.

Gerald V Post and Albert Kagan (2007) 'Evaluating information security tradeoffs: Restricting access can interfere with user tasks', Computers & Security, Vol. 26 (3), May, pp. 229-237 <https://www.hmso.gov.uk/acts/acts2006/pdf/ukpga_20060048_en.pdf>.

Carl Schmitt (1996 [1927]), *The Concept of the Political*, Chicago: University of Chicago Press.

Brett Stalbaum, 'The Zapatista Tactical FloodNet: A collaborative, activist and conceptual art work of the net' <http://www.thing.net/~rdom/ecd/ZapTact.html>.

Iain Thomson (2008) 'Enterprise security software market booms', 18 June <http://www.vnunet.com/vnunet/news/2219275/enterprise-software-market>.

Leon Trotsky (1987 [1911]) 'Terrorism', in 'What do we mean...?', *Education for Socialists: No. 6*, March, Socialist Worker's Party.

Irving Wohlfarth (2009) 'Critique of Violence: the deposing of the law', in *Radical Philosophy*, Jan/Feb: 153, pp. 13-26.

Slavoj Zizek (2008) *Violence*, London: Profile Books.