### 1AC

#### In 1998 four people inspired by the actions of 1960s civil rights activism-Ricardo Dominguez, Brett Stalbaum, Stefan Wray, and Carmin Karasic-founded the Electronic Disturbance Theatre. Their main goal, according to Wikipedia, was to “organize and program computer software to show their views against anti-propagandist and [military](http://en.wikipedia.org/wiki/Military) actions, and begin mobilizing micro-networks to act in solidarity by staging [virtual sit-ins](http://en.wikipedia.org/wiki/Virtual_sit-ins) on-line and allowing the emergence of a collective presence in direct digital actions.” Prior to their formation, hacker culture was entirely anonymous, and the EDT putting themselves out in the open was something altogether new and unexpected.

#### Ricardo Dominguez reflects on this decision-

“I decided that we would become the Electronic Disturbance Theater, and then we made a decision that was very very strange but that seemed on a gut level what we needed to do, but it went against all the usual elements. We decided not to be anonymous. Not to be secret – to be transparent. And this went against hacker culture, which is about anonymity, which is about secrecy. We also pushed open source. That is, all our code had to be very simple, you know, anybody can use it. We would also let people know what we were doing, when we were going to do it, how we were doing it. And I felt this would create a much better drama.”

#### The group worked with the Zapatistas in Mexico and brought down websites of then president Ernesto Zedillo, exposing human rights abuses as well as escalating militarism to the public eye, becoming a crucial part of the toppling of the regime.

#### Their success brought on a new wave of performative hacktivism, its epicenter becoming Austin, Texas-where I live. Groups like the hacktavismos and the Cult of the Dead Cow stood in solidarity with anti-neoliberal movements, providing communication networks for organizations trying to challenge oppression.

#### In 2004, Alexandra Samuel refers to the series of events conducted by the EDT and other organizations as the beginning of performative hacktivism, a new method for 21st century “electronic civil disobedience” and social dissent.

#### She describes performative hacktivism as the use of techniques developed in art, music, and theatre in a way that challenges the new core of civil society—the theatre of cyberspace

Alexandra Samuel, PhD in Political Science, September 2004, “Hacktavism and the Future of Political Participation,” pg. 71-73, DKP

Performative hacktivism consists of legally ambiguous hacktions, undertaken by hacktivists with artist-activist backgrounds. It draws heavily on the tradition of political theater in its adaptation of hacking for political purposes. The term “performative” not only captures the broad notion of hacktivism as performance – which these hacktions most certainly are – but also the more particular idea of political protest as a “speech act”. The notion of politics as spectacle that has informed performative hacktivism also characterizes a wider array of “carnivalesque” protest tactics popularized by the antiglobalization movement (Boje 2001). Many performative hacktivists come from theater or art backgrounds, and see hacktivism as a new form of political art. Some of these hacktivists produce other forms of Internet or digital art, in addition to their hacktivism. And even those performative activists who are not artists per se share the aesthetic and theoretical baggage of the postmodern left. Since performative hacktivism emerges out of a left political culture, we should not be surprised that it usually focuses on left-wing issues such as globalization, liberation struggles (especially that of Mexico’s Zapatistas), and corporate power. Many performative hacktions have been coordinated, or at least timed to coincide, with simultaneous street protests. The most visible groups of performative hacktivists are the Electronic Disturbance Theater, ®™ark, and the electrohippies. The Electronic Disturbance Theater is a group of four U.S.-based activists who banded together in 1998 to create a digital protest in solidarity with the Zapatistas. ®™ark is a U.S.-based activist “mutual fund” that sponsors acts of “anti-corporate sabotage”—including a number of hacktions. ("®™ark Website", “Bringing it to You” page) It uses its status as a legal corporation to both spoof and (potentially) benefit from limitations on corporate liability(Sebok 2001). The UK-based electrohippies collective was created in July 1999 with the intention of using the Internet to challenge the commercialization of cyberspace; until it disbanded in July 2002, it focused its activities on anti-corporate hacktions like its virtual sit-in against the WTO. Performative hacktion**s** have encompassed a wide range of issues, but usually focus on offline issues like globalization and human rights. They almost always engage a transnational coalition of activists, even if the sites are assembled by hacktivists in one country who then solicit sit-in participation from a broader cross-national population. Performative hacktivism mostly takes the form of virtual sit-ins or site parodies – forms of hacktivism with clear precedents in the traditions of street protest and political theater. This area of hacktivism has also made some moves into the field of software development, but only as a way of facilitating the primary tactics of sit-ins and site parodies. The EDT developed an open source version of its sit-in tools, and a group called the Yes Men have created software that automates the creation of web site parodies. While performative hacktivist tactics are carefully constructed to avoid clear legal jeopardy, they are not without legal risk. The virtual sit-in tactic is essentially a less illegal version of the denial-of-service attack; since actual people are loading the pages that overload a server, it is not clearly illegal. But at least one virtual sit-in (conducted by the EDT in 1998) was counter-attacked by the U.S. military (Schwartau 2000), and a site parody (of the WTO’s web site) faced the threat of legal challenge (Ramasastry 2002). The intensity of the reaction that these hacktivists have provoked attests to the success of their hacktions as performance. Performative hacktivists are very much oriented to the public eye, and see their activities as a way of challenging corporate and media domination of public discourse. Their hacktions are aimed at shifting that discourse by raising awareness and creating public pressure – not at directly affecting outcomes. As this may suggest, performative hacktivism is more theory-driven than other forms of hacktivism. Performative hacktivists often cite European critical theorists as sources of intellectual inspiration in their efforts to comprehend the political or performative dimensions of cyberspace: Ricardo Dominguez offers a typical voice when he writes that “[r]ecombinant culture, the implosion of genetics and speed, creates a spasm of hypermorphic delusion wherein Sandborn-understands-Virilio-as-Hegelunderstands- Napoleon.”(Dominguez 1996) Different performative hacktivists offer different theoretical takes on the nature of hacktivism, but a common theme is the way the Internet has changed the relationship between the human body and human identity. Performative hacktivists use the Internet as a way of exploring the new virtual body, and its relationship to the corporeal world; they sometimes argue that power has shifted altogether into the virtual world, and thus needs to be challenged within cyberspace itself. In the opening words of *The Electronic Disturbance*, a theoretical work that has informed the activities of the EDT in particular: The rules of cultural and political resistance have dramatically changed. The revolution in technology brought about by the rapid development of the computer and video has created a new geography of power relations in the first world that could only be imagined as little as twenty years ago: people are reduced to data, surveillance occurs on a global scale, minds are melded to screenal [sic] reality, and an authoritarian power emerges that thrives on absence. The new geography is a virtual geography, and the core of political and cultural resistance must assert itself in this electronic space. (Critical Art Ensemble. 1994, p.3)

#### Although pop culture first romanticized these performers as computer geeks who stole from the rich and gave to the poor, the war on terror ushered in a new security regime that labeled them as terrorists to be feared and eliminated. The media began to turn on these playful artists of cyberspace, demonizing them as threats against national security, and instilling a fear of the dangerous hackers in the minds of the public

#### Peter Krapp explains that,

Peter Krapp, 2003, Synapsis: A Carnivore Client, “Terror and Play, or What Was Hacktivism?” pg. 71, DKP

Pop culture no longer celebrates hacking as the generally innocuous but occasionally very profitable pursuits of the computer hobbyist. As television has stopped romanticizing the obsessions of talented nerds, the press no longer touts the boot-strapping spirit of digital capitalism. Instead, TV and print journalists have been selling the specter of hacktivism as an irreducible systemic threat of digital media…

He continues, saying that-

Peter Krapp, 2003, Synapsis: A Carnivore Client, “Terror and Play, or What Was Hacktivism?” pg. 75-76, DKP

It was the spirit of playful exploration that led to a majority of computer related innovations and business ideas for several decades. Until the late 1980s, a hacker was someone who, by trial and error and without referring to a manual, ended up successfully operating computers. Yet only five years later, experts on computer culture began to warn that hacking posed “a serious and costly problem.”17 For the longest time, commentators on digital culture had focused on access, learning, privacy, and free speech. Yet in a sudden and massive sea change in popular opinion as well as legal and economic policy regarding network technology and education, alarmist commentators began to demonize those who tried to access more than the official, limited interface, at times even suggesting that unruly computer users might end up influencing foreign policy, diplomacy, and international law.18 The Net had promised to turn a medium of distribution back into a medium of communication, as Brecht had demanded of radio.19 But shortly after the end of the Cold War released new media technologies of mass distraction into general circulation, the network was reined in by the trifecta of privatizing the backbone of the Net, closing computer operating systems, and censoring cyberspace. The general direction for achieving this closure appears to be security through obscurity and vilification of anyone who doubts the wisdom of blanket secrecy. This tendency grew only once the messianic promise of e-commerce was debunked, the clipper chip that would have granted federal authorities surreptitious access to all personal computers fended off, and major corporations co-opted the rhetoric, if not the spirit, of open source software. As the promise of an open digital culture yields to a control society where code is law, hacktivism figures as agency panic—as the ill-conceived actions of the disenfranchised in a world divided between placeless power and powerless places. Computer-mediated communication enables marketers and data-mining companies, the U.S. Department of Homeland Security, and its globe-trotting bigger brother, Echelon, to cross-reference and search every imaginable kind of database, combining video and audio surveillance with intercepted Internet traffic, medical end employment records, school and library files, credit ratings, tax and criminal data, shopping and travel patterns, and more. Our only solace might be, as optimists used to argue, “that this personalized inquisition may well have the bludgeoning sophistication and accuracy of customer profile questionnaires”—but for a growing number of people, anonymity in the techno-crowds is an illusion.20 As the citizens of media society grow more transparent, networked power becomes increasingly intransparent, giving rise to conspiracy theories. And no doubt much hacktivism is borne of the same mentality, indulging in fantasies of outright manipulation of the powerless that serve as justification for all manner of attempts to poke holes in the screens of secrecy and to unmask the powers that be.

#### **As society began to see hacktivists as a growing threat to their order, they responded with massive expansions of presidential war powers—the patriot act, the NSA, and a series of secret memos, would construct the new fascistic police-state that expanded their domain to cyberspace**

#### **Paul Roberts explains that secret memos involving the domestic use of offensive cyber operations became the infrastructure of this new policy state**

Roberts 13-former Assistant Secretary of the US Treasury and Associate Editor of the Wall Street Journal, PhD @ University of Virginia, Post-Grad fellow @ Berkeley & Oxford, [Paul, Counter Punch, “The Police State is Real,” 2/8/2013, <http://www.counterpunch.org/2013/02/08/the-police-state-is-real/>, DKP]

The Bush regime’s response to 9/11 and the Obama regime’s validation of this response have destroyed accountable democratic government in the United States. So much unaccountable power has been concentrated in the executive branch that the US Constitution is no longer an operable document. Whether a person believes the official story of 9/11 or not, the result is the same: 9/11 was used to create an open-ended “war on terror” and a police state. It is extraordinary that so many Americans believe that “it can’t happen here” when it already has. We have had a decade of highly visible evidence of the construction of a police state: the PATRIOT Act, illegal spying on Americans in violation of the Foreign Intelligence Surveillance Act, the initiation of wars of aggression–war crimes under the Nuremberg Standard–based on intentional lies, the Justice Department’s concocted legal memos justifying the executive branch’s violation of domestic and international laws against torture, the indefinite detention of US citizens in violation of the constitutionally protected rights of habeas corpus and due process, the use of secret evidence and secret “expert witnesses” who cannot be cross-examined against defendants in trials, the creation of military tribunals in order to evade federal courts, secret legal memos giving the president authority to launch preemptive cyber attacks on any country without providing evidence that the country constitutes a threat, and the Obama regime’s murder of US citizens without evidence or due process. As if this were not enough, the Obama regime now creates new presidential powers by crafting secret laws, refusing to disclose the legal reasoning on which the asserted power rests. In other words, laws now originate in secret executive branch memos and not in acts of Congress. Congress? We don’t need no stinking Congress. Despite laws protecting whistleblowers and the media and the US Military Code which requires soldiers to report war crimes, whistleblowers such as CIA agent John Kiriakou, media such as Julian Assange, and soldiers such as Bradley Manning are persecuted and prosecuted for revealing US government crimes. The criminals go free, and those who report the crimes are punished.

#### And, these secret memos have been directed at domestic targets. OCOs are now used to target domestic leftist activism and manipulate the media to advance neoliberal propaganda.

Global Research 13-[Washington’s Blog, Centre for Research on Globalization, “Global Cyberwarfare. High-Level US Intelligence Source: ‘We Hack Everyone Everywhere’”6/8/2013, <http://www.globalresearch.ca/global-cyberwarfare-high-level-us-intelligence-source-we-hack-everyone-everywhere/5338193>, DKP]

Glenn Greenwald – who broke the phone and internet spying stories this week – has a new exposé … this time on offensive cyber-warfare: Barack Obama has ordered his senior national security and intelligence officials to draw up a list of potential overseas targets for US cyber-attacks, a top secret presidential directive obtained by the Guardian reveals. \*\*\* An intelligence source with extensive knowledge of the National Security Agency’s systems told the Guardian … “We hack everyone everywhere. We like to make a distinction between us and the others. But we are in almost every country in the world.” \*\*\* The full classified directive repeatedly emphasizes that all cyber-operations must be conducted in accordance with US law and only as a complement to diplomatic and military options. But it also makes clear how both offensive and defensive cyber operations are central to US strategy. Under the heading “Policy Reviews and Preparation”, a section marked “TS/NF” – top secret/no foreign – states: “The secretary of defense, the DNI [Director of National Intelligence], and the director of the CIA … shall prepare for approval by the president through the National Security Advisor a plan that identifies potential systems, processes and infrastructure against which the United States should establish and maintain OCEO capabilities…” The deadline for the plan is six months after the approval of the directive. The directive provides that any cyber-operations “intended or likely to produce cyber effects within the United States” require the approval of the president, except in the case of an “emergency cyber action”. When such an emergency arises, several departments, including the department of defense, are authorized to conduct such domestic operations without presidential approval. Obama further authorized the use of offensive cyber attacks in foreign nations without their government’s consent whenever “US national interests and equities” require such nonconsensual attacks. It expressly reserves the right to use cyber tactics as part of what it calls “anticipatory action taken against imminent threats”. The directive makes multiple references to the use of offensive cyber attacks by the US military. Greenwald and others have long reported that the Obama administration claims the right to be judge, jury and executioner in both drone assassinations and offensive cyber attacks. Greenwald also reports that the head of the cyber command is the NSA boss … the same guy responsible for much of the spying we’ve been hearing about: In January, the Pentagon announced a major expansion of its Cyber Command Unit, under the command of General Keith Alexander, who is also the director of the NSA. That unit is responsible for executing both offensive and defensive cyber operations. (There are other overlaps and interconnections between spying and warfare as well.) The War Comes Home Offensive cyber operations are not only occurring overseas … The Department of Defense has long waged cyber-war against Americans by censoring and manipulating social media and other websites. More proof here and here. This is not entirely surprising, given that: Programs which the government claims are aimed at foreign entities have long been used against American citizens living in the United States The “war on terror” has come home. If the government claims the power to assassinate and indefinitely detain American citizens living on U.S. soil … it’ s not going to hesitate in targeting them for propaganda and cyber-warfare The government has long sought to spread propaganda through mainstream media, video games, movies, television, and every other popular medium. Famed Watergate reporter Carl Bernstein says the CIA bought and paid for many successful journalists. See also this New York Times piece, this essay by the Independent, this speech by one of the premier writers on journalism, and this and this roundup . And the CIA is investing in technology which lets them cut out the middle man altogether … by having a computer write news stories On the other hand, real reporters who criticize those in power are being harassed, targeted and smeared Government agencies are scouring the Web for any critical comments about them, actively manipulating social media for propaganda purposes, and to help the too big to fail businesses compete against smaller businesses (and here ), and to promote viewpoints which have nothing to do with keeping us safe

#### **Policy has moved beyond just solidifying military dominance and strategic operations. It has resulted in the shutdown of any meaningful debate over OCOs and war powers. Obama has shrouded new cyber policy in secrecy, and fighting back against this censorship is a pre-requisite to assessing the effectiveness of these operations**

#### This is Kevin Gosztola writing for *The Dissenter*, in 2013

**Back in November 2012, the Washington Post reported on a “secret” presidential directive that President Barack Obama had signed and characterized it as “the most** extensive White House **effort to date to wrestle with what constitutes an ‘offensive’ and a ‘defensive’ action in the rapidly evolving world of** cyberwar and cyberterrorism.” **This cybersecurity directive, which was classified “top secret,” has been published by The Guardian‘s Glenn Greenwald and is the latest in a series of leaks on government surveillance. The directive reads: …The Secretary of Defense, the DNI, and the Director of the CIA – in coordination with the AG, the Secretaries of State and Homeland Security, and relevant IC And sector-specific agencies – shall prepare for approval by the President through the National Security Advisor a plan that identifies potential systems, processes, and infrastructure against which the United States should establish and maintain OCEO capabilities; proposes circumstances under which OCEO might be used; and proposes necessary resources and steps that would be needed for implementation, review, and updates as US national security needs change. [Action: DoD, Office of the DNI, and CIA update to Deputiess on scope of plans; 6 months after directive approval]… OCEO or Offensive Cyber Effects Operations are defined as “operations and related programs or activities other than network defense, cyber collection or DCEO [which are Defense Cyber Effects Operations] — conducted by or on behalf of the United States government, in or through cyberspace, that are intended to enable or produce cyber effects outside United States Government networks.” “Cyber effects” is essentially a sanitized term developed by the Obama administration, similar to “enhanced interrogation techniques” or “kinetic operation,” that is used when referring to acts of cyber warfare. According to the directive, “The United States Government shall identify potential targets of national importance where OCEO can offer a favorable balance of effectiveness and risk as compared with other instruments of national power, establish and maintain OCEO capabilities integrated as appropriate with other US offensive capabilities and execute those capabilities in a manner consistent with the provisions of this directive.” It would presumably give the Obama administration more ability to conjure up legal justifications to continue to engage in cyber attacks against the critical infrastructure of Iran. This policy also provides guidance on when cyber warfare operations could be launched in the domestic United States. “Until such time as any additional criteria for domestic operations are approved by the President, authorization by department and agency heads for Emergency Cyber Actions that are intended or likely to produce cyber effects within the United States (or otherwise likely to adversely affect US network defense activities or US networks) shall be granted only if the President has provided prior approval for such activity,” according to the directive. And, if the president doesn’t approve, there are other “constraints” in the policy that supposedly define how to proceed. When the Post** [**reported**](http://www.washingtonpost.com/world/national-security/obama-signs-secret-cybersecurity-directive-allowing-more-aggressive-military-role/2012/11/14/7bf51512-2cde-11e2-9ac2-1c61452669c3_story.html) **on this directive, it was presented as something to help make cybersecurity more efficient and ensure that “US citizens’ and foreign allies’ data and privacy are protected and international laws of war are followed.” It was presented as a directive intended to institute a process for vetting “operations outside government and defense networks.” And, it does set out some parameters for doing that, but it also was designed to make it more possible to wage offensive cyber operations. Also, in looking this over, it does not appear to include any mention of any sources or methods that agencies would use for operations. Specific details of how defensive or offensive operations would be carried out are not described. How agencies would cooperate with one another is suggested and what would be done to review operations and keep them within the boundaries of the law. So, the “top secret” classification would seem to be improper and it would seem to be reasonable to contend this kind of directive should always be made public by presidents who issue them. As I** [**highlighted**](http://dissenter.firedoglake.com/2012/11/14/obamas-secret-directive-keeps-evolving-cybersecurity-policy-concealed/) **back in November, this directive updated one by President George W. Bush that has remained secret. Bush issued sixty-six national security directives.** [**At least thirty**](http://www.fas.org/irp/offdocs/nspd/index.html) **of them are still classified. Obama has issued twenty presidential policy directives.** [**Only five**](http://www.fas.org/irp/offdocs/ppd/index.html) **them are public. Steven Aftergood of Secrecy News has** [**urged**](http://niemanwatchdog.org/index.cfm?fuseaction=ask_this.view&askthisid=00321) **Obama to release a “summary account” of each of the national security directives Bush signed, which remain secret: …Of the 54 National Security Presidential Directives issued by the (George W.) Bush Administration to date, the titles of only about half have been publicly identified. There is descriptive material or actual text in the public domain for only about a third. In other words, there are dozens of undisclosed Presidential directives that define U.S. national security policy and task government agencies, but whose substance is unknown either to the public or, as a rule, to Congress… One might recall Obama said** [**in his first days of office**](http://www.fas.org/blog/secrecy/2009/01/a_new_era.html) **his presidency was “the beginning of a new era of openness in our country.” He told reporters, “For a long time now there’s been too much secrecy in this city.” He paraphrased former Attorney General John Ashcroft and said, “The old rules said that if there was a defensible argument for not disclosing something to the American people, then it should not be disclosed… That era is now over.” He claimed his administration would be on the side of those that seek to make information known and he would hold himself to a ‘new standard of openness.’ Quite the opposite has occurred, as Obama has embraced a new standard of secrecy by seeking to carve out national security exceptions or exemptions in policies intended to protect whistleblowers or journalists or encourage transparency in government. He has embraced the Bush tactic of invoking the overly broad “state secrets” privilege in order to prevent the declassification or exposure of information. He has fought efforts by the American Civil Liberties Union to make public secret legal interpretations or opinions that form the basis of policies around the US’ “targeted killing” program and its interpretation of Section 215 of the PATRIOT Act (the “business records” provision). He has zealously pursued alleged leakers or whistleblowers, even as his administration regularly discloses classified or sensitive information to major newspapers like the New York Times or the Washington Post. And, he’s presided over a government with a rampant overclassification problem that has only festered and opened criminal investigations into reporters and media organizations for publishing previously classified information, including the Associated Press, Fox News reporter James Rosen and WikiLeaks. Furthermore, Obama claims to “welcome” debate, but that rhetorical posture sharply conflicts with the actions or record of his presidency. He has not wanted the press or public to debate because the Executive Branch is to set the national security policies and Congress is to be informed when the president decides to inform them and federal judges are not to make decisions about whether policies are lawful or not because the Obama administration sees having their power checked as an infringement on their authority to expand the national security state without any limitations whatsoever.**

\*cite for above\* Gosztola 13-writer, artist, performer and activist [Kevin, The Dissenter, “Top Secret Cybersecurity Policy Directive Revealed & the Debate Obama May ‘Welcome’ But Never Have,” http://dissenter.firedoglake.com/2013/06/08/top-secret-cybersecurity-policy-directive-revealed-the-debate-obama-may-welcome-but-never-have/, DKP]

#### These directives are specifically intended to crack down on internal dissent

This is Martin in 13-Writer @ Global Research-Centre for Research on Globalization [Patrick, Global Research, “Obama’s ‘Cyberwarfare First Strike’: Using Offensive Cyber Effects Operations (OCEO) to Destabilize Countries,” 6/10/2013, http://www.globalresearch.ca/obamas-cyberwarfare-first-strike-using-offensive-cyber-effects-operations-oceo-to-destabilize-countries/5338457, DKP]

The directive [Presidential Policy Directive-20] also discusses possible cyber attacks by the US government against domestic targets inside the country. This raises the prospect that in the event of a political crisis in the US, stemming either from domestic political and social upheaval or mass opposition to war, the US government could shut down the Internet and social media, target specific web sites or carry out other acts of cyber warfare in the name of “national security.”

#### Apocalyptic rhetoric of cyberwarfare is at the heart of cybersecurity politics—the question of predictions being accurate takes a backseat to escalating threats in hopes predictions will someday become true

Stevens, 13Tim Stevens, Prof. at , King’s College London Department of War Studies “Apocalyptic Visions: Cyber War and the Politics of Time” <http://s3.amazonaws.com/academia.edu.documents/31124211/Apocalyptic_Visions_-_Stevens_14-04-13.pdf?AWSAccessKeyId=AKIAIR6FSIMDFXPEERSA&Expires=1377455187&Signature=xLDiNWVoQar2i4n0aIHuBof7maw%3D&response-content-disposition=inline>

 **Apocalyptic thinking is inherently eschatological**, **interpreting history through the prism of finitude**: contemporary events are imbued with eschatological meaning and are interpreted as ‘signs’ of impending apocalypse (Robbins and Palmer, 1997: 4-5). **The roll-call of signs of cyber war will b**e familiar: Cuckoo’s Egg, Eligible Receiver, Morris Worm, ILOVEYOU, Code Red, **Estonia, Georgia**, 7 Conficker, Operation Aurora, **Stuxnet**, Flame, Duqu, and so on. This **litany of signs**—although internally heterogeneous—**imparts metonymic gravitas to cyber war narratives** and fulfils a significant mnemonic function in reminding audiences continually of the seriousness of cyber threats. **They become ‘signifiers of the no-longer-future-but-reality of cyber-war’** (Cavelty, 2013). **Their historical specificity is elided in their construction as discrete events, the frequency of which is**   **always increasing** (e.g. Herrera-Flanigan, 2013), and which lead inevitably to cyber war. **Prophets who read and pronounce upon these apocalyptic signs**—the ‘Cassandras of cyber warfare’ (Rid, 2012: 6)—**do not**, like their religious counterparts, **restrict themselves to specific dates and**   **times** upon which terrible events will occur, **so need not excuse themselves from incorrect**   **predictions**; consequently, **they can never be wrong**. However, they do have in common talents as ‘masterful bricoleurs, skilfully recasting elements and themes within the constraints of their respective traditions and reconfiguring them to formulate new, meaningful endtimes scenarios’ (Wojcik, 1997: 148). **Specific vectors of ‘cyber insecurity’ may change, and timescales expand and**   **contract, but the certainty in apocalypse remains unwavering**. ‘**Apocalyptic intensity’** **is maintained** **and** **heightened** further **by making continued ‘imminent but indeterminate’ predictions**, **legitimising**   **a constant state of readiness in which adherents ‘feel themselves to be standing poised on the brink**   **of time’** (Bromley, 1997: 36). In fact, it is always ‘only a matter of time’ before a ‘cyber-apocalypse’ occurs (Gable, 2010). This uncertainty is shared with other forms of security, which thrive on a ‘denotative imprecision …. simultaneous appeal to the hard and the vacuous, the precise and the imprecise …. vague generalities about everything and nothing’ (Walker, 1997: 63). This epistemic tension is partially resolved by reading the signs of cyber war as corroboration of a deterministic ‘script’ of the future (Robbins and Palmer, 1997: 5). When events and scenarios converge, the narrative of cyber war gains explanatory power in its own right. In periods of ‘thickened history’ like this, it becomes ever more difficult to comprehend these events—‘to see the wood for the trees’, as 8 it were—and they become part of their own causal structure (Beissinger, 2002: 27). In this case, the impression is that if cyber war is not already occurring, it very soon will be. The initiation of the apocalypse is frequently reduced to the familiar digital motif of a finger hovering above the button or positioned in readiness for a final, decisive mouse-click or emphatic keystroke: ‘There was a time when war was begun with a shot. Now it can begin with the simple click of a mouse. A silent attack that you may never even know occurred until it all unfolds in front of you’ (Rudd, 2011). During the early Cold War, the image of the US president’s finger poised above a ‘nuclear button’ became the standard symbol of state military power (Strong, 2005: 34) but in an age of cyber war, the power to foment societal chaos is available to all: as UK armed forces minister Nick Harvey warned, ‘the finger hovering over the button could be anyone from a state to a student’ (Hopkins, 2011). The difficulties of representing cyber threats visually (Hansen and Nissenbaum, 2009: 1165) partially explain the popularity of this imagery but like the nuclear case—for which substantial visual resources were available—there is semantic power in this reduction of immense sociotechnical complexity to a simple manual action (Plotnick, 2012). Like the informational bits mediating the human will to prosecute these actions, the decision to proceed is also binary: on/off, yes or no. **We might never know who hit us or why but this single physical act brings the future**   **rushing catastrophically into the present, the moment of ‘cosmic ecstasy**’ (Chernus, 1982) **in which**   **all apocalyptic predictions are validated**. **This suggests apocalypse is also an object of desire, something to be welcomed and, perhaps,**   **brought into being** (e.g. Cook, 2004). Apocalypse is not merely the end but also a beginning, a time of both revelation and transformation. An apocalyptic belief in the transformation of the human condition through catastrophe informs the rhetoric of, for instance, the US-led ‘war on terror’ as much as it does the jihadism of those who prompted it (McLaren, 2002; Jackson, 2005: 103-105), even if the utopian ideal of achieving a ‘terror’-free world is as unlikely as Islamist dreams of global 9 caliphate (Gray, 2007). They remain visions no matter how hard one strives to achieve them and are part of a ‘catastrophic’ strand of apocalypticism, pitting good against evil and privileging dystopian and pessimistic views of human nature (Wessinger, 1997). **Cyber war scenarios frequently express**   **this catastrophic apocalypticism, yet these eventualities are not entirely unwelcomed**. **Cyber war as**   **apocalypse is ‘an illumination unveiled precisely at the very moment of the greatest darkness and**   **danger’** (Aho, 1997: 65), a light to dispel the night of political foot-dragging and insufficient cyber security. The catastrophic materialisation of the ‘virtual’ threat is the necessary catalyst through which to achieve this transformation. In this respect, apocalypse operates in its primary sense of ‘revelation’, a ‘singular instant both revealing the meaning of the past and announcing the future’ (Bousquet, 2006: 756), in this case the political errors of the past and the sunlit uplands of a ‘cyber secure’ future. Understood not only as catastrophe but as the revelatory wellspring of transformation, apocalypse need not be wholly negative. Millennial beliefs in better futures are by no means exclusive to religion, amply demonstrated by scientific movements like eugenics, cryonics and space exploration, which share a conviction humankind can be transformed and improved through technology (Bozeman, 1997). The posthumanist movement, specifically in its attention to the coming ‘technological singularity’ is overtly apocalyptic but also emphasises the positive social benefits an information-technological transformation will bring (DeLashmutt, 2006). The technological singularity may be a violent rupture but not necessarily; it may, some argue, have happened already—we just didn’t notice. 2 **Apocalypse need not be catastrophic but can be ‘progressive’,**   **affirming collective cooperation in bringing about earthly salvation** (‘progress’) **without the radical**  **violence of divine retribution** (Wessinger, 1997). **These utopian and transformative impulses are in a**   **long lineage of technoscientific thought, expressing secular rather than religious apocalypticism** 2 This issue is also raised with respect to cyber war: ‘**what if we were at war and didn’t know it?**’ (Brenner, 2009: 100).10 (Hughes, 2012). **How else is apocalyptic cyber war located with respect to this spirit of apocalyptic**   **modernity and postmodernity**?

#### The collusion of the state, the military, and corporations has pushed its way into cyberspace. Resisting this fascism is the only way to stop the mass slaughter of the increasingly omnipotent war machine

Deleuze and Guattari 80 (Gilles, professor of philosophy at U of Paris Vincennes, and Felix, psychoanalyst and political activist, A Thousand Plateaus Pg. 230-231)

This brings us back to the paradox of fascism, and the way in which fascism differs from totalitarianism. For totalitarianism is a State affair: it essentially concerns the relation between the State as a localized assemblage and the abstract machine of overcoding it effectuates. Even in the case of a military dictatorship, it is a State army, not a war machine, that takes power and elevates the State to the totalitarian stage. Totalitarianism is quintessential conservative. **Fascism** on the other hand **involves a war machine**. When fascism builds itself a totalitarian State, it is not in the sense of a State army taking power, but of a war machine taking over the State. A bizarre remark by Virilio puts us on the trail: **in fascism, the State is** far less totalitarian than it **suicidal**. **There is in fascism a realized nihilism.** Unlike the totalitarian State, which does its utmost to seal all possible lines of flight, **fascism is constructed on an intense line of flight, which it transforms into a line of pure destruction and abolition**. It is curious that from the very beginning **the Nazis announced to Germany what they were bringing: at once wedding bells and death, including their own death**, and the death of the Germans. **They thought** they would perish but that **their undertaking would be resumed**, all across Europe, **all over the world, throughout the solar system. And the people cheered** not because they did not understand, but **because they wanted that death through the death of others.** **Like a will to wager everything you have every hand, to stake your own death against the death of others**, and measure everything by "deleometers." Klaus Mann's novel, Mephisto, gives samplings of entirely ordinary Nazi speeches and conversations: "Heroism was something that was being ruled out of our lives…. In reality, we are not marching forward, we are reeling, staggering. Our beloved Fuhrer is dragging us toward the shades of darkness and everlasting nothingness. How can we poets, we who have a special affinity for darkness and lower depths, not admire him? . . . **Fires blazing on the horizon; rivers of blood in all the streets; and the frenzied dancing of the survivors, of those who are still spared, around the bodies of the dead**!"32 **Suicide is presented** not as a punishment but **as the crowning glory of the death of others**. One can always say that it is just a matter of foggy talk and ideology, nothing but ideology. But that is not true. **The insufficiency of economic and political definitions of fascism does not simply imply a need to tack on vague, so-called ideological determinations.** 'We prefer to follow Faye's inquiry into the precise formation of Nazi statements, which are just as much in evidence in politics and economics as in the most absurd of conversations. They always contain the "stupid and repugnant" cry, **Long live death**!, even at the economic level, where the arms expansion replaces growth in consumption and where investment veers from the means of production toward the means of pure destruction. Paul Virilio's analysis strikes us as entirely correct in defining fa**s**cism not by the notion of the totalitarian State but by the notion of the suicidal State: **so-called total war seems less a State undertaking than an undertaking of a war machine that appropriates the State and channels into it a flow of absolute war whose only possible outcome is the suicide of the State itself,** "The triggering of a hitherto unknown material process, one that is limitless and aimless. . . . Once triggered, its mechanism cannot stop at peace, for the indirect strategy effectively places the dominant powers outside the usual categories of space and time. ... It was in the horror of daily life and its environment that Hitler finally found his surest means of governing, the legitimation of his policies and military strategy; and it lasted right up to the end, for the ruins and horrors and crimes and chaos of total war, far from discharging the repulsive nature of its power, normally only increase its scope. Telegram 71 is the normal outcome: If the war is lost, may the nation perish. Here, Hitler decides to join forces with his enemies in order to complete the destruction of his own people, by obliterating the last remaining resources of its life-support system, civil reserves of every kind (potable water, fuel, provisions, etc.)."33 **It was this reversion of the line of flight into a line of destruction that already animated the molecular focuses of fascism, and made them interact in a war machine instead of resonating in a State apparatus. A war machine that no longer had anything but war as its object and would rather annihilate its own servants than stop the destruction. All the dangers of the other lines pale by comparison.**

#### Therefore, David and I advocate the use of performative hacktivism as a method for countering offensive cyber operations

#### Hacktivists are at the front of the global information war—revolutions against state oppression are grounded in cyber space

Penny 11-writer, journalist and activist who writes regularly for The New Statesman and the Independent, author of books about dissent [Laurie, The Nation, “Cyberactivism From Egypt to Occupy Wall Street,” 10/31/2011, [http://www.thenation.com/article/163922/rise-digital-natives#](http://www.thenation.com/article/163922/rise-digital-natives), DKP]

Like so much on the Internet, in a way, contemporary hacktivism started with porn. Anonymous, for example, originated in the chat site 4chan, whose message boards are scurrilous back-channels full of filthy in-jokes. Early DDoS attacks, starting in February 2010, targeted Australian authorities who tried to censor the distribution of cyberporn—a project code-named Operation Titstorm—as well as a proxy company that attempted to bring down The Pirate Bay, a file-sharing site for downloading music and videos. At stake was not so much nude photos or free MP3s but the very principle of free information exchange. In this sense, **the trajectory of hacktivism from defending free file sharing to defending freedom itself may have been inevitable.** “It started off with exposing titty videos to their friends,” explains one member of the militant “tech dissent” collective DSG (Deterritorial Support Group), who identifies as Zardoz. “It ended with bringing down [an] autocratic regime.” He (or she) is referring to the Egyptian revolution, a key moment of politicization for **cyberactivists, who stepped in to help the rebels with communications after** Hosni **Mubarak shut down the Internet.** As the Arab Spring and subsequent global upheaval of the summer demonstrated, **the fight for freedom of speech and action online has become enmeshed with the offline struggle for freedom of movement and thought. The “politicization of 4chan,”** as this trajectory is partially known among hacktivists, **can be traced to WikiLeaks.** After the whistleblowing website released thousands of classified documents and diplomatic cables last fall, **MasterCard and PayPal announced they would suspend payments to WikiLeaks, prompting members of Anonymous to shut down the companies’ websites.** Titled Operation Payback, **the project changed the rules of engagement for those cyberactivists who had previously seen their anticensorship activities as separate from geopolitics.** In this sense, WikiLeaks’s great triumph has been to make the world think again about whether governments should have the right to withhold information from citizens and obstruct the free exchange of ideas online. For young people around the world who grew up with the Internet—“digital natives”—the question is both profound and profoundly uncomplicated. **Defending the freedom to share information online is more important than individual politics or morality. “That’s why Anonymous intervened in Wikileaks,”** explains Zardoz. “That’s why they intervened in **Tunisia. And** that’s why they intervened in **Egypt.” In Operation Egypt and Operation Tunisia, Anonymous and other groups coordinated to restore citizens’ access to websites blocked by the government.** The efforts extended beyond the Internet, with faxes used to communicate vital information as a means of last resort. (In classic “lulzy” style, cyberactivists also caused havoc by ordering enormous quantities of pizza delivered to Egyptian and Tunisian embassies.) **After Egypt, it became clear that the fight against censorship and the fight against state oppression were moving closer together. “This is not a minor struggle between state nerds and rogue geeks,”** wrote members of the DSG collective in June, in an influential blog post titled “Twenty reasons why it’s kicking off in cyberspace.” **“This is the battlefield of the 21st Century, with the terms and conditions of war being configured before our very eyes.”** On this point, hacktivists and security experts agree. “LulzSec and Anonymous are exposing the huge number of vulnerabilities that are out there waiting to be exploited by someone who has the skills and the motivation,” says Chris Wysopal, co-founder of Veracode, a security company based in Massachusetts. **“Data is so leaky,”** says NYU’s Coleman, **“and if all you need to crack a government facility is a USB stick, can we really stop that happening?”**  **That’s precisely the question that has state powers running scared.** In these unsteady times, one of the few things we can know with any certainty is that the future is digital; the Internet—and the possibilities for collective engagement and disruption it offers—is not going away. It would take a massive worldwide program of censorship and surveillance both on- and offline to crack down on this, and that’s just what “tech dissidents” are hoping to prevent. \* \* \* **The link between dissent by technology and dissent in the streets is growing stronger. The fact that ordinary citizens can get and share information instantaneously not only provides them with the tools to resist authority and evade arrest; it also delegitimizes that authority on practical and philosophical levels. Controlling information**, after all, **is one of the most important ways a state wields its power.** Over nineteen months that have seen the nature and structure of power called into question around the globe, **the nature and structure of technological dissent have grown and matured in kind.** To police, the press and the powerful, this evolving link between technology and dissent is cause for alarm: **nobody knows what cyberactivists might be capable of next.** Ultimately, **one person’s cyberterrorist is another person’s digital freedom fighter**, and for many, that’s precisely what hacktivists are. In Liberty Plaza, the nerve center of the Occupy Wall Street protest is a makeshift media tent full of serious young people fussing over laptops in tangles of cables. Not all cyberactivists are young—stereotyping hacktivists as adolescent recluses is an easy way to dismiss their ideas—but there’s one thing that teenagers and technologies can do far faster than grown-ups and governments, and that’s adapt.

#### The hacktivism embraced by the affirmative is the civil disobedience of our age. Our generation has been shaped, controlled, and dominated by cyberspace. Access to flows of information is the new currency of elite power, rupturing these lines of communication is the only way to challenge the new era of fascism

This is Nozomi Hayase in 2013-contributing writer to Culture Unplugged, global citizen blogger @ Journal Between Words, she brings out deeper dimensions of socio-cultural events at the intersection between politics and psychology to share insight on future social evolution, PhD Candidate in Philosophy [Nozomi, Counter Punch, “Manning, Snowden and Assange, The Rise of the Internet Dissidents,” 8/13/2013, [http://www.counterpunch.org/2013/08/13/the-rise-of-the-internet-dissidents/,](http://www.counterpunch.org/2013/08/13/the-rise-of-the-internet-dissidents/%2C) DKP]

NSA whistleblower Edward Snowden’s volcanic revelations of ubiquitous US surveillance are in their third month. The aftershocks felt around the world continue. As Russia granted Snowden temporary asylum, the White House fell into anger and dismay.¶Computer scientist Nadia Heninger argued that **leaking information is** now **becoming the “civil disobedience of our age”. The late historian and activist Howard Zinn described the act of civil disobedience as “the deliberate, discriminate, violation of law for a vital social purpose”.** He advocated it saying that **such an act “becomes not only justifiable but necessary when a fundamental human right is at stake and when legal channels are inadequate for securing that right”.**¶ Snowden’s act was clearly one of civil disobedience. John Lewis, US Representative and veteran civil rights leader recently noted that **Snowden was “continuing the tradition of civil disobedience by revealing details of classified US surveillance programs”.**¶ Snowden is not alone. In recent years, **there have been waves of dissent that revealed the depth of corruption and abuse of power endemic in this global corporate system.** Before Snowden, there was Bradley Manning and Jeremy Hammond who shook up the trend of criminal overreach within the US government and its transnational corporate and government allies. Private Bradley **Manning blew the whistle on US war crimes and** activist Jeremy **Hammond exposed the inner workings of the pervasive surveillance state**. They took risks to alert the world about the systemic failure of representative government and the trend toward a dangerous corporate authoritarianism.¶ After Snowden was charged with espionage, WikiLeaks founder Julian Assange called for global support to stand with him:¶ “Edward Snowden is one of us. Bradley Manning is one of us. They are young, technically minded people from the generation that Barack Obama betrayed. **They are the generation that grew up on the Internet and were shaped by it….”**¶Snowden, Manning and Assange are all part of an Internet generation **that holds that** **transparency of governments and corporations is a form of check and balance on power. They believe in the power of information and in the public’s right to know.** In an interview with Glenn Greenwald of The Guardian, **Snowden described how his motive was “to inform the public as to that which is done in their name and that which is done against them.” He advocated for participation of ordinary people in decision-making processes** as a vital part of democratic society **indicating that the policies of national security agencies that he exposed should be up to the public to decide.** This belief is shared by his forerunners.¶ Manning, who inspired Snowden, wrote in his infamous chat log with ex-hacker Adrian Lamo: **“I want people to see the truth… regardless of who they are… because without information, you cannot make informed decisions as a public.”** He confirmed this conviction once again when he testified at the providence inquiry for his formal plea. After admitting that he was the source of the largest leak of classified information in history, he spoke again about the motivation behind his actions:¶ “I believed that **if the general public**, especially the American public, **had access to the information … this could spark a domestic debate on the role of the military and our foreign policy in general.”**¶ In pleading guilty to one count of conspiracy for hacking into the computers of the private intelligence firm Stratfor, computer whiz Jeremy Hammond stated that he believed, **“People have a right to know what governments and corporations are doing behind closed doors”.**¶ Barrett Brown, journalist and director of a website called Project PM, which crowd-sourced information exposing the activities of the cyber-intelligence industry, also held a similar conviction. Brown now sits behind bars with a possible maximum sentence of 105 years for his daring investigation of the growing private intelligence contractor industry. In an interview with NBC’s Michael Isikoff, **Brown described “information freedom” as “the value of this age”. He spoke of how this belief motivates many cyber-activists to engage in civil disobedience against those in positions of power who act unethically.**¶ **The motto of these activists is: privacy for the public, transparency for government officials and corporate executives.** It was this care for privacy and protection of personal information that motivated Snowden to risk his freedom and also caused Andrew ‘Weev’ Auernheimer to expose a security flaw inside AT&T servers. “Auernheimer’s crime was not a hack” Natasha Lenard of the Salon clarified his position. She explained how “he did not illegally access a private server. Rather, his conviction hinged on what data gets to be authorized or unauthorized and who gets to decide this”. Though his actions didn’t harm anyone, Auernheimer was sent to prison for pointing out the company failure to protect user’s data.¶ **It is this common theme of information freedom that motivates this new generation of activists. Their fight against a corrupt system required great personal sacrifice; they have been incarcerated, stripped naked, put on show trials, stuck in an airport transit space and immobilized in an Ecuadorian embassy.**¶ A Vision of a New World¶ **These digital dissenters speak truth to power. By way of the new digital medium, they revealed the deep fraud of an arrogant system that enables governments and corporations to look into the private lives of others while concealing their own immoral actions from the public. But, this was not all; these young activists also saw a vision of a new world and of a more open and just society.**

#### Nozomi continues, arguing that controlling information is the primary way corporations, militaries, governments, and the elite maintain their power over the masses. Our dissent is a way of turning the weapons of the elites against them, building new lines of communication between people in a way that embodies a collective consciousness powerful enough to topple regimes of domination. What is allowed in debates has been censored and controlled, the aff busts those information pipelines open and allows for emancipatory change.

Hayase 13-contributing writer to Culture Unplugged, global citizen blogger @ Journal Between Words, she brings out deeper dimensions of socio-cultural events at the intersection between politics and psychology to share insight on future social evolution, PhD Candidate in Philosophy [Nozomi, Counter Punch, “Manning, Snowden and Assange, The Rise of the Internet Dissidents,” 8/13/2013, [http://www.counterpunch.org/2013/08/13/the-rise-of-the-internet-dissidents/,](http://www.counterpunch.org/2013/08/13/the-rise-of-the-internet-dissidents/%2C) DKP]

Before Snowden’s whistleblowing, Julian Assange saw the increasing force that was subverting the internet and alerted people to the spying networks created by transnational corporate allies. In the book Cypherpunks: Freedom and Future of the Internet, co-written with Andy Müller-Maguhn, Jérémie Zimmermann and Jacob Appelbaum, Assange showed how **the internet can be used as an instrument for both freedom or oppression.**¶ “Once upon a time in a place that was neither here nor there, we, the constructors and citizens of the young internet discussed the future of our new world,” Assange wrote in the introduction. **Pioneers of this net culture seemed to have recognized a democratizing force inherent in the technology of the internet and how its power, when truly freed, could transform the existing structures of control and ownership.** The founder of WikiLeaks articulated the vision of Cypherpunks, a group of activists who woke up to the potential of cryptography in bringing societal and political change:¶ **“We say that the relationships between all people would be mediated by our new world, and that the nature of states, which are defined by how people exchange information, economic value, and force, would also change. We saw that the merger between existing state structures and the internet created an opening to change the nature of states. … The new world of the internet**, abstracted from the old world of brute atoms, **longed for independence …”** Assange saw how **the internet** is moving in a manner contrary to his vision and how it “**has been transformed into the most dangerous facilitator of totalitarianism we have ever seen” and indeed has become “a threat to human civilization”.** He elaborated in a Guardian article how the control of oil resources has been a major denominator for granting certain countries geopolitical power and “**the war for oil pipelines**” has been driving the world. He explained how now this battle **has shifted over into “the war for information pipelines: control over fibre-optic cable paths that spread undersea and overland”.**¶ Now, **the situation is accelerating.** In the last couple of years **we have seen a tremendous assault on internet freedom. The force to squash the vision of this generation has infiltrated cyberspace. The battle has begun.**¶The Frontier of Digital Liberation¶ **The trend toward centralized control or restriction of information flow has become an antithesis to the way of life experienced by this generation of digital activists.** Richard Stallman who inspired figures like Assange also warned about the surveillance scheme. Stallman, a founder of the Free Software Movement, promotes freedom respecting software, which gives users control over their technology. **He pointed to an unfolding battle between corporations and a growing body of people who believe software and communication venues should be free of insidious covert control.** He described how this control is exercised by a form of propriety where, for example corporations and governments subjugate users with insidious features such as converting cell phones into spying and tracking devices and creating software backdoors to make changes to programs or install intentionally malicious software without user’s consent.¶In the name of copyright and intellectual property, the act of sharing has in many cases become a crime, yet some have found creative ways to circumvent the systemic clampdown. One of those on the frontier of digital liberation is Gottfrid Svartholm Warg, alias anakata, a Swedish computer specialist who co-founded the BitTorrent site The Pirate Bay, which facilitates peer-to-peer file sharing. Similar pioneering work was done by Kim Dotcom, a German-Finnish Internet entrepreneur who launched the Hong Kong- based company Megaupload, which enables massive file storage and viewing. Such actions were legally attacked by the corporate-government information cartels. Svartholm Warg was charged with illegal downloading of copyrighted material and sent to jail, while the US government overextended its arrogant imperial power byattempting to shut down Megaupload and extradite founder Dotcom.¶ While the founder of Pirate Bay sits behind bars, Torrent Site continues to combat the censorship. It is releasing a customized Firefox called PirateBrouser that enables users to go around the censorship. After the stories of NSA mass spying became public, Dotcom announced the upcoming release of an encrypted secure message apps and email service. He stated that he might move this privacy service overseas to Iceland, which is known as a strong advocate for protesting citizen’s privacy.¶ Now, more people are joining together to defend the values of the Internet generation. In the last few years, the online collective Anonymous has become the ubiquitous face of cyber-activism. With V for Vendetta “Guy Fawkes” masks, this loosely tied decentralized network acts whenever and wherever their radar catches classic abuses of power. They fiercely mobilize to take on the powerful, whether it is arrogant government contractors like Aaron Barr, religious organizations like Scientology, child sexual abusers or immoral governments and corporations. “Beneath this mask there is an idea …” They are united with shared sense of justice and conviction that “ideas are bulletproof”. Repeatedly, Anonymous has shown to be a champion of the downtrodden and those that challenge illegitimate power.¶ Ideals of the Heart¶ **The common struggles in what these young people are fighting against bind them together, but the true mark of this generation is a shared vision of a world with virtues like sharing, love and creativity that have been suppressed in the trend toward extreme capitalism within the transnational corporate-state.**¶ **Along with a new found courage, these young people reveal a strong sense of compassion and trust in ordinary people.** In the online chat logs, **Manning** showed his extraordinary empathy for others when he **wrote, “I can’t separate myself from others … I feel connected to everybody… like they were distant family.”**¶ At OHM 2013, a five day outdoor international festival for hackers and cyber security workers, retired CIA officer Ray McGovern remarked how both Snowden and Manning acted with empathy when they witnessed human suffering. They trusted the general public over governments and found hope in the actions of ordinary people to change the course of society for the better. Manning said:¶ **“… its important that it gets out … I feel**, for some bizarre reason … **it might actually change something … hopefully worldwide discussion, debates, and reforms … if not… than we’re doomed as a species.”**¶ The same sentiment was shared by Snowden when he said, **“The greatest fear that I have regarding** the outcome for America **of these disclosures is that nothing will change”. It is those human attributes that the empire is trying to punish.**¶ On July 30th, the military judge delivered a verdict in the case of Bradley Manning. Manning was not found guilty for the most ridiculous charge of “aiding the enemy” for leaking state secrets and evidence of war crimes that were published by major news outlets and posted on the internet. Yet, he was found guilty of multiple counts including six Espionage Act offenses. He faces punishment of up to 136 years in prison, which during the sentencing phase, was reduced to maximum of 90 years.¶ In responding to the verdict, journalist Norman Solomon wrote about how the problem the U.S. government had with **Manning** was that he **acted out of “caring, with empathy propelling solidarity”.**¶ Darker Net called for a miracle in the freeing of Bradley Manning, ringing a similar note:¶ **“The US Government wants to lock him away forever. Why? Because he had compassion. Because he had a profound sense of justice. Because he understood the difference between right and wrong. Because he saw aspects of war that horrified him. Some might say he had an innocence; was naive. But perhaps if we all had that same innocence, the world might be a better place.”**¶In this sense of naïveté there lies a strength that makes it possible for us to act toward a vision of a world that we imagine. “It takes a little bit of naivety in order to jump in and do something that otherwise looks impossible. Many great advances in science, technology and culture have a touch of naivety at their inception”, WikiLeaks wrote in their about page describing how the organization was first formed.¶ What at first appears as naïveté is what plants seeds for higher ideals. Sharon Staples, who helped care for Bradley Manning when he was a child, recalled her interaction with him when she visited him in Fort Leavenworth, Kansas: “I asked him if he wanted me to send him anything and he said, ‘Everything I want is in here and here.’ …. As he said the word ‘here’, he pointed to his head, then his heart.”¶ Ideals grow in the minds and hearts of many in this generation and help cultivate a moral sensibility that allows each person to make unique contributions to the world. Janet Reitman, who wrote a defining piece on Hammond, ended the article by highlighting Hammond’s idealism, “He was an idealist who even after being jailed kept fighting at every occasion and he never betrayed himself”.¶ **For those in power, the idealism of this generation and their conscience is an existential threat to their order. The ‘crime’ of aiding the enemy here is really the act of aiding democracy and acting for the public good. In the end, it has shown that we the public have become the enemy of the state.**¶ Austrian philosopher Rudolf Steiner said of the younger generation:¶ “The question is not: what knowledge or skills does a person need to have in order to benefit the existing social order. But: what pre-disposition does this person have, and what is capable of development? Then it would be possible to channel new energies from the rising generation into the social order. Then the rising generation will not be fitted into the mould of the existing society, rather society will be what these newly recruited adults make of it.”¶ **What is really happening with the growing trend of crackdowns on dissents and truth-tellers? Our society has failed to listen. Those in power are actively shutting out the voices of those with conscience.** Obama’s unprecedented war on whistleblowers and equating these heroic deeds with treason are simply a symptom of this deafening of society. How did we get to this place? How has our society become so degraded?¶ We Are Winning¶ This totalitarian surveillance state wasn’t built in a day. There was a warning. Back in 1975 the late Senator Frank Church at the famous Church Committee hearings challenged the burgeoning potential of total surveillance in the US:¶ “[The National Security Agency's] capability at any time could be turned around on the American people, and no American would have any privacy left, such is the capability to monitor everything: telephone conversations, telegrams, it doesn’t matter. There would be no place to hide”.¶ 38 years later, this young courageous whistleblower stepped forward to once again alert the people of the world to the severity of Big Brother moving into a digital dystopia, which he assessed as “turnkey tyranny”. All the US government would need to do would be to give the order and this once-great nation would spiral into overt despotism.¶ **The battle continues in earnest between two forces; freedom and control, transparency and secrecy, sharing and proprietary ownership. It is in this fight that the Internet generation has found itself.**¶ Speaking from the Ecuadorian embassy, Assange said, “We are winning … We are a part of a new international body politic that is developing, thanks to the internet”. He predicted to see the inevitable defeat of the national security state, saying that young people of ages between 20 and 30 are the ones who are recruited into the NSA and the CIA and those who are exposed to the Internet are shaped by certain values. He said that they will find “the agencies that they work for do not behave in a legal, ethical or moral manner.” **This is already happening and this new form of information dissent is spreading.**¶ For instance, at the Black Hat conference, a gathering of computer experts and cybersecurity professionals in Las Vegas, NSA head Keith Alexander was repeatedly interrupted by the audience. As Alexander stated NSA’s mission for freedom, a critical voice emerged to oppose the NSA surveillance.¶ Despite Obama’s aggressive prosecution of whistleblowers, the climate of fear doesn’t seem to hinder the will of those who act with conscience**.** Edward Snowden spoke of how he learned from others who came before him and that the power of ones conscience is something that cannot be imprisoned or stopped:¶ “Binney, Drake, Kiriakou, and Manning are all examples of how overly-harsh responses to public-interest whistle-blowing only escalate the scale, scope, and skill involved in future disclosures. Citizens with a conscience are not going to ignore wrong-doing simply because they’ll be destroyed for it: the conscience forbids it. Instead, these draconian responses simply build better whistleblowers.”¶ **The recent Snowden asylum victory is just the beginning. Debates over reform are happening. Now privacy has a chance to at least have a front seat debate. Snowden’s revelations led to a major House vote on an amendment that would defund one single NSA program** to end their blanket collection of US phone records. **Even though the bill was defeated**, it was lost by only 12 votes. **It brought huge shifts in public opinion about the security state and government secrecy. A grassroots organization called “Restore the Fourth” quickly formed,** which had its first round of protest on July 4th to challenge the unconstitutionality of NSA mass surveillance after it was revealed by Snowden. **The group recently launched mass protest**s, calling for “1984 Day”, named for George Orwell’s classic novel about a Big Brother surveillance state. **This movement is gathering momentum. Across the US in major cities, people marched calling to end the government spying.**¶ The founder of a US-based encrypted email service, reportedly used by Edward Snowden, Ladar Levison announced he was shutting down the operation. The decision was made after being given a difficult choice between becoming “complicit in crimes against the American people” or walking “away from nearly ten years of hard work by shutting down Lavabit.” He chose the latter instead of submitting to US government’s secret order to give them access to customer content.¶ **While government surveillance brings pressure on internet companies to collude with them, more and more people are coming together to resist this insidious force.** Three of Germany’s largest email providersannounced their plans to partner up to strengthen the security of messages sent between them. Mailpile, an Iceland-based free/open source email service is crowd-funding a secure private email client/cloud service that is an alternative to US-tied services such as gmail. After the revelation of the Xkeyscore spying program that is shown to specifically target Wikipedia users, the WikiMedia foundation stepped forward to take extra measures to protect users privacy.¶ **Nothing can stop this generation infused with a new sense of justice and shared vision for humanity.** Similar to online connections, where when one link is broken, another emerges; **when one person is taken out, several more emerge because courage is contagious. This desperate empire might stop one individual, but it cannot lock them all up.**¶ **Call them whistleblowers, dissidents, hackers or geeks, the youth of today’s Internet generation is uncovering for the world the level of deceit and corrupted state power.** **Our connections, our genuine care for one another is a power in the ether and creates a network that can lead us into a future that is imagined in our collective heart. Whether or not this generation can help move the world beyond the inhumane system of illegitimate governance is up to us, as we too are a part of this rising Internet generation.**¶ **The battle has begun.**