IMMATERIAL CIVIL WAR: THE WORLD WIDE WAR ON THE WEB

Harry Halpin

Introduction

As the online world has become increasingly the locus of collective intelligence - a concept I will discuss in more detail shortly - the once relatively peaceful and obscure backwaters of Internet governance have been wracked by what can only be termed a new world war, albeit one that is invisible. It is an immaterial civil war. The term 'immaterial civil war' refers to the fact that this war is between forces that both threaten to tear a nearly invisible – immaterial – Internet architecture apart, and an ethical conflict between the generations where the new digital natives have a distinct form of life from that of their forebears. At stake is the future of digital sovereignty: who creates the protocols, who assigns the names and numbers, that enable communication and give existence to objects on the Internet? Perhaps even more importantly, the very future of collective intelligence can be said to be at stake. Will the Internet be allowed to expand as a space for the free sharing of digital information, or will restrictions from various pre-Internet institutions be imposed upon the Internet itself? Will the Internet create its own revolutionary forms of social self-organization, or usher in a new regime of personalized surveillance? The answers to these complex and threaded questions escape easy judgment. Nevertheless, one thing is certain: the actions that determine their answers for future generations will be decided within this decade.

The Thesis of Immaterial Civil War

Until recently, the Internet as a globe-spanning 'network of networks' seemed to exist purely as a technical space, a nearly magical ether that could deliver any kind of information to anyone at

anytime – at least ideally. In reality, the uneven development of Internet access meant this was not always the case. As noted by Alan Kay, 'the Internet was done so well that most people think of it as a natural resource like the Pacific Ocean, rather than something that was man-made. When was the last time a technology with a scale like that was so error-free?' (quoted in Binstock, 2012). This view of the Internet as a natural resource is illusory, however, for the Internet achieves its stunning technical interoperability and equally stunning global penetration by virtue of committing to a digital peace treaty brokered by the complex social network of interlocking and sometimes even inimical institutions who control the technical infrastructure. This 'peace treaty' was accomplished technically by having these institutions deploy a series of standardized protocols that respected a few general social principles. The common protocols, ranging from TCP/IP to HTML, were created and are currently maintained by the 'immaterial aristocracy', flesh-and-blood human agents who professionally create and maintain these protocols in standards bodies. 'Some of these are hackers, while others are government bureaucrats or representatives of corporations – although it would seem that hackers usually create the protocols that actually work and gain widespread success. To the extent that those protocols are accepted, this class that I dub the 'immaterial aristocracy' govern the net' (Halpin, 2008). They operate via a small number of standards bodies, such as the IETF (Internet Engineering Task Force), or the W3C (World Wide Web Consortium), multi-stakeholder protocol governance bodies that allow individual or institutional participation with a large degree of informality, democracy, and consensus-driven decision making process, all with little or no official governmental status. It is the duty of these immaterial aristocrats to preserve, in the form of technical standards, the often inarticulate guiding ethical principles, such as net neutrality, that are conjectured to have led the Internet to its astounding growth. Their success so far cannot be underestimated: the Web as it stands today is the largest informational artifact in human history.

Yet the peace treaty of protocols is increasingly being torn apart in a 'World War 3.0' between the present immaterial aristocracy and an alliance of repressive government regimes working hand-in-hand with the telecommunication corporations (Gross, 2012). Interestingly, when it comes to challenging the immaterial aristocracy the instrument of choice is the ITU, the International Telecommunications Union (ITU), which is a U.N. agency where only nation-states have a deciding vote. The stakes are high for all

sides: as dramatically witnessed by the 2011 Tunisian revolution and the destruction of the traditional music business over the last decade, many pre-Internet institutions are having their very existence placed at risk by the possibility of the free and uncensored sharing of information that is potentially enabled by the Internet. The existence of the standards bodies, non-profits, and corporations that have long held immense power over the Internet is equally at stake. Since its inception the rather ad-hoc technical hegemony of the primarily American immaterial aristocracy has never before been globally challenged in the realm of realpolitik. If those bodies fail to rise to the occasion, this aristocracy will no doubt lose their digital sovereignty to define protocols and thus their raison d'être for existence. Nowhere has this struggle taken on such symbolic significance as at the ITU's World Conference on International Telecommunications (WCIT) on December 3-14th, 2012, which – strangely enough – took place in a desert governed by an authoritarian regime. Yet against the expectations of many (such as Michael Gross), the future of the Internet was not decided in the air-conditioned nightmare of Dubai – it was rather postponed.

Although almost no major changes to Internet governance came from the much-heralded Dubai WCIT conference, this does not mean the immaterial civil war over the control of the Internet is over. Far from it. This war is now rapidly transforming into a conflict: not between pre-Internet institutions and the open Internet, but between the very corporations that championed the open Internet against the ITU and their own users. So far we have seen only early skirmishes of what may be a decade-long struggle for control over the Internet. It is therefore of the highest theoretical and strategic importance to begin to think through what is at stake for the future of the Internet as a global commons, including the history and motivations of the various actors in this conflict and their battles.

This crucial task is motivated by the fact that so far the Internet remains a medium for the growth of collective intelligence. Collective intelligence is an often-used term that is difficult to pin down precisely. It can be understood variously as referring to: an aggregated swarm in contrast with a lone individual; an individual in contrast with the larger (often technical) cognitive scaffolding of a highly technical society; or the individual node in a network contrasted with a large network that any particular node subsides within. While defining collective intelligence precisely is beyond the scope of this essay, the inference is hopefully clear: collective

intelligence can be thought of as a particular kind of distributed cognitive system that is self-maintaining (or more precisely, autopoietic) in the face of often unpredictable problems. The theory of distributed cognition, as pioneered by cognitive anthropologists such as Hutchins (1995), points out that 'groups may have cognitive properties that differ from those individuals who constitute the group', where cognitive properties refer to memory and attention. For example, a group of sailors can pilot a ship only by virtue of their co-ordination via technical artifacts and social co-ordination. However, distributed cognition may also be autopoietic in the sense used by Maturana, forming 'a circular organization which secures the production or maintenance of the components that specify it in such a manner that the product of their functioning is the very same organization that produces them' (Maturana & Varela, 1973: 48). The classic example deployed by Maturana is that of the reproduction of the cells that maintain the existence of an animal such as a biological frog. Maturana also strongly opposes the addition of technical or social components to an autopoietic system. In marked contrast to the biological grounding of Maturana, in this essay I will follow Hutchins by hypothesizing that such self-maintaining systems may include both people and technical infrastructure, meaning groups of humans coordinating over the Internet can be considered a form of autopoietic collective intelligence.

In the peculiar frame of reference given by what I am here calling the immaterial civil war over the Internet, the problem-solving capacities of collective intelligence are far beyond those of individual humans, and the infrastructure to harness these collective capabilities is laid by the technical protocols and infrastructure that compose the Internet. The Internet gains its power by virtue of being a genuine extension of our problem-solving capacities via a trusted technical substratum open to all. Yet, depending on the results of this immaterial civil war, we risk the Internet being transformed into a foreign and hostile power capable of turning our own collective cognitive powers against us and towards goals inimical to our future survival, ranging from pure profit to total social control.

The thesis is that this immaterial civil war is both real and ongoing, and will be the defining war of the next decade. There are two obvious objections to this idea. First, that the term 'immaterial' is an objectionable misnomer, with certain unfortunate Cartesian connotations that are simply unnecessary when it comes to engaging

with the true content of immaterial labor: the centrality of information and communication to production in the 21st century. Yet even this term 'immaterial' has an element of truth in it, for it is the case that most of us cannot 'see' the dissemination of information on the Internet, as it consists of a flow of packets of data in TCP/IP across heterogeneous networks, and so what could be termed 'immaterial' is perhaps more properly regarded as 'invisible.' In other words, we no longer see the wires. Indeed, we have difficulty imagining what it would mean to 'see' bytes in-and-of-themselves. Our everyday experience of the Internet is increasingly delivered through wireless frequencies meant for mobile phones. Yet this apparent invisibility is layered upon a robustly material infrastructure: the majority of the high-speed 'backbone' of Internet-enabled networks consists of fibre-optic cables buried underground that wind their way through various regional exchanges, creating a hidden infrastructure much like a nervous system across the planet. It is precisely this materiality that allowed former Egyptian president Mubarak to infamously 'shut down' the Internet by closing off only a few access points in 2011. Wireless frequencies, while imperceptible to our eyes, are perceptible to our devices and consist of very real electro-magnetic fluctuations in our environment. The truth latent in the term 'immaterial' is that the material terms are secondary: as I have shown in detail elsewhere, information can only be realized in a substratum that is capable of supporting the requirements for digitality (Halpin, 2013). The distinguishing characteristic of information is that the 'same' information on a level of abstraction can be realized across wireless broadband, fiber-optic cables, and perhaps even in the human brain itself. I will therefore persist with the term 'immaterial' insofar as it refers, however imperfectly, to the digital nature of information and the primacy of the meaning – and thus the syntax and semantics – of protocols, in contrast to 'material' implementation details.

The second and more serious objection that can be made to the idea that immaterial civil war is both real and ongoing, and will be the defining war of the next decade, is to claim that it is pure hyperbole to declare a state of war over the Internet, as such a statement does immense injustice to the blood and dirt of material war. In popular imagination, war is thought of as being confined to various state actors who fight over material resources; in this respect, the U.S. invasion of Iraq, with its all-too-obvious goal of domination over oil production and the placement of military bases with client regimes near geopolitically strategic axes, could be considered exemplary. This is not to deny that in every war there has always been an

informational component - in terms of a battle for 'hearts and minds' - and so the justification of war in terms of propaganda, ranging from Helen of Troy to weapons of mass destruction, is as old as war itself. Yet until recently it has been difficult to imagine a war that would take place purely in the space of information, a seeming ethereal realm where there are no bombs and charred remains. Conceiving our own times using a mental model derived from industrial or even Napoleonic war, however, represents something of a failure of imagination. Wikileaks, whose release of information was interpreted by the U.S. government as an act of war, offers an obvious example. Perhaps more fitting still is that provided by China's rather explicit 'hacking war' against the United States government and its corporations. By employing intelligence information and the capture of source code, this state-sponsored hacking has enabled the former to deliver 'trade secrets' to Chinese corporations. Indeed, Richard Clarke, a U.S. Government cybersecurity advisor for thirty years, has stated that every U.S. corporation has been penetrated by such Chinese hacking attacks - while remaining not-surprisingly mute on the number of compromised U.S. government installations (Protalinski, 2012). As the seemingly immaterial realm of codes, signs, and affects becomes increasingly central to the existence of power, it is therefore possible to see the Internet as simply another terrain of war, with governments today having to formally open a division of cyberdefense on a par with the navy and army, just as they once had to formally acknowledge the existence of the sky as a battlefield with the creation of national air forces.

This leads to a disturbing implication of immaterial civil war, one that demonstrates how immaterial information is layered onto a material substratum – that immaterial war may actually precede material war. As noted by Alexander Galloway in his analysis of Debord's Kriegspiel, a precondition to a successful operation in warfare consists in maintaining control over lines of communication as much as control over space: 'The key is the network of lines of communication, a detail of game design entirely lacking in a game like chess. Superimposed on the game board, the lines simulate the communication and logical chains of campaign warfare; Debord's rules stipulate that all pieces on the board must stay in contact with a line, else risk destruction' (Galloway, 2009). At the same time we should not deny the role played by the fundamental transition of late capitalism in all this: namely, the fusion of material resources with cybernetic protocols that creates value-chains of production and consumption that not only cover the earth like a vast vibrating spider

web, but use these protocols to react 'just in time' to changes in supply and demand. These protocols are run over the Internet, of course; therefore control of these protocols is essential in any material war. This is the new geopolitics in the virtual space of the Internet. Immaterial war over the control of protocols may be just setting the stage for material war, and so the spectre of the failure of the Treaty of Versailles lurks in the shadows over Dubai.

In order to fully explain the hypothesis of immaterial civil war and its ramifications for collective intelligence, I want to begin by interrogating both the battle over an exemplary principle of the Internet – net neutrality – and the governmental and corporate actors that wish to overthrow it. This interrogation will reveal how an alliance of the immaterial aristocracy, Silicon Valley, and of Internet users, won this particular battle. The next horizon of struggle on the Internet with which I want to engage is the capture of personal data by platforms. (Is there is a danger here of conforming to perhaps too-classical a Hegelian dialectic: one whereby, in the first moment, the users of the Internet identify with their masters in Silicon Valley in the fight against an external enemy; and then, in the second moment, they realize their own latent power?) Finally, I want to look at some of the wider repercussions of this immaterial civil war: namely, how it has been participated in to an unimaginably large extent. What I want to analyze in particular is the potential for a future where digital natives recognize the importance of the Internet to their own powers of collective intelligence, and create structures of self-organization that may truly be fitting for coming generations.

The Battle of Net Neutrality

In the first battle of the immaterial civil war during 2011, many users of the Internet supported Silicon Valley in their fight against the international regulation of the Internet. The long-standing immaterial aristocrats were viewed from this perspective as mediating the desires of ordinary users against various shifting alliances between repressive governments such as Russia and China – as opposed to the United States, which in general supported the immaterial aristocracy. To really understand this struggle, however, it is necessary to delve into the origins of the very historically peculiar governance of the Internet by the immaterial aristocracy. The original foundations of the immaterial aristocracy lie with the Internet Engineering Task Force (IETF), the de-facto standards-setting body for the Internet. Reflecting its informal foundation in

an eclectic group of graduate students and enthusiasts involved in creating the software that ran the early Internet in the 1960s (government sub-contractors usually stuck to hardware), the decisions of this body are made by 'rough consensus and running code' (Halpin, 2008). In fact, the vast majority of the actual decisions are made over mailing lists, although on the rare occasions the IETF meet in person, consensus is taken by humming. In this way the IETF define the rules of protocols such as TCP/IP via RFCs, or 'Requests for Comments' publications. While the RFCs are quite technical and dry, guiding principles that give the Internet a unifying architecture are nonetheless present in these documents. Perhaps one of the most surprising guiding principles is that of network neutrality.

IETF RFC 1958, rather grandly entitled the 'Architectural Principles of the Internet,' states that 'the current exponential growth of the network seems to show that connectivity is its own reward' (Carpenter, 1996). The RFC claims this success is due to the Internet's implementation of the 'end to end argument,' which is summarized as 'certain required end-to-end functions [that] can only be performed correctly by the end-systems themselves' (Carpenter, 1996). As a matter of technical exegesis, what this means is that the network should be neutral and transparent and simply route packets of data to end-points, such as browsers and servers, and thus not inspect the content of any data traveling through the Internet. The principle further states that 'end-to-end protocol design should not rely on the maintenance of state (i.e. information about the state of the end-to-end communication)' (Carpenter, 1996). As a result, any preferential treatment or blocking of network traffic between the nodes (such as the client web browser and the server web server) violates the end-to-end principle. Violations of net neutrality that normally take the form of ISPs would likely have to engage in some level of deep packet inspection, the explicit search through the data packets sent through the Internet by the ISP. On the Internet, however, a strange technical version of universal rights for data reigns, as all data should be treated equally. This design decision was taken, not for ethical reasons, but for the mundane technical reason of keeping debugging network traffic errors simple. As stipulated by the original designers of TCP/IP like Vint Cerf, 'Black boxes would be used to connect the networks; these would later be called gateways and routers. There would be no information retained by the gateways about the individual flows of packets passing through them, thereby keeping them simple and avoiding complicated adaptation and recovery

from various failure modes' (Leiner et al., 2003). Shockingly, what the original Internet engineers had accidentally stumbled upon in net neutrality was a powerful source of what has been termed 'generativity', namely that 'system's capacity to produce unanticipated change through unfiltered contributions from broad and varied audiences' (Zittrain, 2008: 70). It is this generativity that allows the Internet to fully exploit what is informally known as Metcalfe's law, the hypothesis that the value of a network is proportional to the square of the number of nodes, which would be endpoints in this case. If endpoints on the network are not equal, the value would also thereby decrease. This principle seems to be as close as one comes to a universal law of what makes networks powerful, from the Internet to almost any network, including Ethernet networks and social networks.

What was not anticipated by the original creators of the Internet was that it would be extended beyond its role in transmitting scientific information (and the sending of messages in military scenarios, as justified in its original budget,), to become a universal medium for any content, converging music, video, television, movie, and gaming. Sharing of content for free, as exemplified by the peer-to-peer BitTorrent protocol, soon blindsided many large multi-national corporations. This lack of foresight has proven increasingly fatal to pre-Internet businesses, in the ironically labeled 'creative' or 'content industries', whose profits are based on their control of content. Such control is difficult if not impossible to maintain digitally - especially when, for every scheme to enforce their control, it seems an 18-year hacker (often from Sweden) will break whatever copyright protection has been baked into software or even hardware within days. Given that they are unable to technically enforce their control of copyright content, it should come as no surprise that many such businesses have turned to government regulations to guarantee their profits. Their goal has become the government regulation of internet service providers (ISPs), in particular the ability to block access to copyright content.

The Internet, despite all the hype from cultural theorists (and even hackers) who consider it to be some kind of magical peer-to-peer system, has a key point of centralization: the assignment of IP addresses and the governing of the top-level domain name system (DNS). The centralization of the domain name system was thoroughly critiqued by Galloway and many hackers, although they seemed to have missed the importance of IP address assignment (Halpin, 2008). Unlike the rather anarchic and directly democratic

process of the IETF, these day-to-day functions of the most valuable resources of the Internet - the granting of names and numbers that give existence itself on the Net - are not autonomous or globally governed democratically. Rather, they are governed *de jure* by the US. Government. To explain in brief, IP addresses are the numbers, like 152.2.210.122, that allow communication on the Internet, while domain names are human readable names, such as 'http://www.ibiblio.org', that a domain name server maps to an IP address. The assignment of IP address blocks and the management of the top eight level domain names servers is carried out currently via IANA (The Internet Assigned Numbers Authority), but was formerly administered personally by the long-bearded IETF volunteer Jon Postel, from the birth of the Internet to his death in 1998. The U.S. Government granted a monopoly on the domain name system to Network Solutions in 1995, letting them charge users for a domain name. Postel envisaged a more democratic system of assigning domain names and numbers, but his proposal for IANA to replace the monopoly of Network Solutions led to a threat to exile him from the Internet, and eventually perhaps his death from a broken heart.. Network Solutions would however later lose its contract, with responsibility moving to ICANN, the Internet Corporation for Assigned Names and Numbers, which is run with an advisory committee of 110 member states and rotating global public meetings. The group accredits for-profit registrars to sell domain names. Yet ICANN still gives the U.S. Department of Commerce final oversight, and it is through this weak point that the so-called 'creative industries' launched their first battle to end network neutrality. By using laws such as the infamous Digital Millennium Copyright Act's 'takedown' notice in the USA and similar laws in other countries, various creative industries attempted to 'block' access to domain names, with their first and primary target being the 'Pirate Bay' BitTorrent file-sharing website. These patchwork attacks to remove content from the Net could be easily circumvented as they operated on an ad-hoc national rather than uniform global level like the Internet.

Thus, the next battle in the war over the Internet was an attempt to place the domain name system under the control of strict copyright enforcement in the form of the now infamous SOPA (Stop Online Piracy Act) bill in the United States Congress. This bill would have forced ISPs to filter out requests for content that might infringe copyright, ominously requiring them to record the IP address of the user requesting such content. The U.S. government would thus have coerced ISPs to intercept and redirect DNS requests for websites

that were claimed to be involved in piracy, in essence causing all ISPs to break net neutrality. The immaterial aristocrats at the IETF were outraged by such a technically ill-guided proposal. The IETF envisaged it would fracture the current centralized control of the domain name system (as users went out of the US to find domain name servers), and that it would violate their plans to secure the domain name system via encrypted authentication by forcing redirection at the level of the ISP. As the IETF pushed their ties in cybersecurity and the military to kill SOPA, outrage against SOPA spread to internet users themselves and Anonymous began attacks on the domain names of prominent backers of the bill. Other websites that felt they might easily fall victim to SOPA, most famously Wikipedia, carried out an 'internet blackout'. Instead of the Wikipedia page, users in the United States got a notice to 'Imagine a world without free knowledge' and a request to contact their U.S. Government. As lawmakers across the political spectrum were flooded with thousands of angry voters demanding they vote to stop SOPA, the bill was quietly withdrawn. It appeared that an alliance of Internet users and companies had won, while the IETF, ICANN, and the rest of the immaterial aristocracy remained in control.

What had failed on a national level was next taken to a global level in the form of ACTA (Anti-Counterfeiting Trade Agreement). This was a secretive multi-lateral global agreement fashioned in much the same way as the traditional globalization agreements that had provoked so-much protest from activists at the turn of the millennia in Seattle, Quebec, and beyond. Although ACTA was officially secret, its contents were leaked to Wikileaks in 2008, and it quickly became apparent that ACTA would also essentially force all agreeing bodies to pass SOPA-like laws to punish ISPs that allowed pirated content. In essence, it would again mandate the destruction of network neutrality, with countries like Japan and the United States having by this time already signed. While the immaterial aristocrats at the IETF seemed to be caught off-guard by ACTA, and companies like Google were forced by governments into non-disclosure agreements, the internet users themselves emerged as a powerful third force at multiple levels, both in traditional government and on the streets. The key battleground became Europe, as ACTA was due to be ratified by the European Parliament. Out of the struggles over the Pirate Bay, various Pirate Parties formed to elect representatives to government to defend their ability to copy files over the Internet, and inside the European Parliament they placed the 21-year old Amelia Andersdotter as their representative from Sweden. As ACTA was debated inside the

Parliament, outside activist groups like Quadranature La Net, led by Jeremie Zimmerman (a friend of Julian Assange) began a public campaign. At first no one seemed to notice, but then as stated by co-founder of Quadranature La Net, Philip Aigrain, 'Anonymous showed up' (personal communication, 2012). Under the banner of the infamous Guy Fawkes mask, the largest demonstrations since the fall of the Communist Regime rocked Eastern Europe, with tens of thousands of people in the streets in Poland and Bulgaria. Cities which had not seem demonstrations in decades, like Iași in Romania, were surprised by the sudden re-appearance of politics in the streets. Bowing to pressure from their constituents, first Poland refused to sign ACTA, with members of Polish Parliament infamously dawning Guy Fawkes masks. Then, finally, in July of 2012, ACTA was defeated in the European Parliament, with the vast majority voting against. While the immaterial aristocrats had always found themselves as the *Geheimsrat* of governments, it appeared that the internet users were able to mobilize to 'hack' democracy itself in order to preserve their founding principles including net neutrality.

An alliance to challenge the immaterial aristocracy more directly was also brewing. This was conceived in order to attack them not only on the level of copyright but also to use the mandate of the United Nations to take away their informal digital sovereignty. Two other forces, besides the industries of content control, had it in their best interest to unseat the immaterial aristocracy. The first was the telecom operators. Often national monopolies or direct descendants thereof, for the last century many telephone operators have been making hefty profits from extracting rent from the usage of their telecommunications lines. This was, until recently, enacted by forcing users to pay exorbitant prices for telephone use, in particular text messages, which cost telco operators virtually nothing. Yet with the rise to maturity of voice-over-IP applications such as Skype, and text-messaging rapidly being replaced by apps such as Wazzap, profits at the large telecom operators had plummeted. There was little or no reason for most users to ask anything from telecom operators except for unlimited mobile internet access, in effect reducing them to a more modest role of ISP. Together with the content industries, the telecoms thus imagined a world where they could violate network neutrality and ask for premium rates for high-speed access to copyright protected content. Strangely enough, while nation-states – with the noticeable exception of China – had for the last two decades routinely ignored the control of the Internet, the wave of revolutions in places such as Tunisia and Egypt, and their subsequent reverberations in places as far apart as Russia and

the United States, had left many governments demanding increased control of the Internet. Interestingly, China used the selfsame technology as was proposed in SOPA and ACTA, domain name blocking and deep-packet inspection, to create the 'Great Firewall of China,' and other countries such as Iran and Pakistan were doing the same. It was just that, while SOPA and ACTA hoped to build a great firewall around copyright content, these governments were endeavouring to construct a firewall around subversive political content.

An unholy alliance was thus struck to destroy the immaterial aristocracy via one of the most 'noble' bodies of global governance, the United Nations. Enter the ITU. The International Telecommunications Union began its life as the International Telegraph Union, a body conceived to unify telegraph communications across national borders, and was eventually subsumed into the United Nations. In marked contrast to the immaterial aristocracy, rather than being composed of individuals like the IETF or organizations like the W3C, only nation-states can vote in the ITU. Despite its admirable goal of 'connecting the world,' especially helpful for developing countries, the ITU quickly came to be seen as a vehicle whereby many authoritarian and repressive regimes were able to get their way. For example, as the body that governs international telephone operations, the assignment of country codes naturally falls under the purview of the ITU. Yet when the People's Republic of China joined the United Nations and ITU in 1971, it deftly used its newfound status at the ITU to remove Taiwan's country code, as Taiwan still claims to be part of China. Taiwan spent years in a strange limbo as a result, wherein it no longer had an international area code, and thus could not be reached in a uniform manner from other countries. Eventually, employees of the ITU friendly to Taiwan managed to give them the reserved 886 calling code that did not officially belong to any country. This of course greatly angered Beijing, which made sure to replace the employees with an emissary of the Chinese government. One of the reasons the US-backed IETF internet protocols succeeded - because attempts by the ITU to develop its own computer networking protocols, the X.800 series of protocols, were both delivered years late and technically inferior to the protocols developed by the IETF – can be considered another point in the ITU's favour.

The ITU planned to take control of the Internet by revising the International Telecommunication Regulations to expand its

definition of telecommunications to include the Internet. This was to be ratified at their WCIT conference in Dubai in 2012. Under the plan the IETF would be abolished, and the role of ICANN in governing DNS would be challenged. An anti-imperialist narrative was quietly manufactured, with the Mali-born engineer Hamadoun Touré leading the developing world against the United States for the control of the Internet, although it would be quietly ignored that the main backers were China, Iran, Russia, and a horde of petty African dictators that they could use to win votes. One proposal was an internet 'tax' to fund increased connectivity in the developing world. But the real story was cybersecurity, re-branded as 'cyberpeace' by the ITU. What this meant was that to end Anonymous (and also, copyright infringement and political dissent), all internet connections had to be traceable to real names by governments via deep-packet inspection. When a joint proposal between the Arab states, China, and Russia was leaked to the specialized WCITleaks.org site, it revealed that the WCIT wanted to put the Internet under total control, so that 'internet governance [would] be effected through the development and application by governments.' The alliance of standards bodies such as the IETF, W3C, and IEE made a weakly-phrased 'Open-Stand' statement to preserve the bottom-up 'multi-stakeholder' process of the immaterial aristocracy. Vint Cerf, now working at Google and the Internet Society (a non-profit body for the IETF), attended as part of the United States delegation. When the ITU formally mustered a last-minute vote to extend its control to the Internet, the United States and its mainly European allies, hand-in-hand with Vint Cerf and the rest of the founding fathers of the Internet, simply walked out: an unprecedented event that in effect killed the ITU as a global process for control of the Internet.

The Coming Battle over Personal Data

In the second moment of struggle over Internet governance, that concerning the capture of personal data, it appears that users are finally recognizing Silicon Valley may be their enemy, and that the immaterial aristocracy are no longer able to mediate between users and the various platforms on the Net. The question today then is: Is it possible that while Internet users may have won the above first battle over net neutrality, they have ultimately lost the war in a manner they failed to anticipate? After all, the real victory in this battle did not belong to them, but to a few multinational Internet corporations, primarily from the United States. To deepen the irony,

these multinationals are ostensibly profiting from the free labour of these selfsame users, and yet claim to represent not only a free and open Internet, but the users themselves against meddling governments. Despite this grand rhetoric, where a shareholder-run company ostensibly 'represents' its labour, it is simply in the economic self-interest of these corporations to keep the Internet out of government control – or at least in the laissez-fair control of the United States government. To take Google's case as a paradigmatic example: it is the ease with which users can violate copyright that keeps users returning to Google's YouTube, and so increasing the profits Google makes by selling advertisements to users and other kinds of personal data. To take another case in point, Google championed net neutrality for many years, and the United States government itself was almost ready to endorse network neutrality by convening all American wireless providers for an agreement. However, in a behind-closed-doors deal it struck with Verizon, it was in Google's best interest to end its commitment to network neutrality for the most important networks of all, mobile networks. Speculation is rife, but already it is clear that Google's attempt to build its mobile Android platform to challenge Apple may require at the very least cutting such deals with Verizon. In a remarkable about-face, Vint Cerf, who besides being the inventor of TCP/IP is also a Google employee, suddenly stopped championing network neutrality openly. A close inspection of the United States position at WCIT in Dubai shows that Internet Freedom in reality means freedom for the market, and the fact is that the market may require some of the fundamental principles of the Internet to be ditched. This brutal reality is not grasped by many of those who hailed the victory over the ITU as a victory for the free and open Internet.

It almost goes without saying that life on the Internet is increasingly captured in a few dominant platforms. As Bruce Sterling put it, 'In 2012 it made less and less sense to talk about the Internet, the PC business, telephones, Silicon Valley, or the media, and much more sense to just study Google, Apple, Facebook, Amazon, and Microsoft' (Sterling, 2012). Forget the ITU, due to sheer market dynamics, each of these platforms is both aiming to control the Internet, and already has control of some of its key infrastructure: browsers, smartphones, search engines. Of course, a classical economist who still believes in the grand fiction of Schumpeterian 'creative destruction' would see no reason why another company could not appear to knock one of these five titans off their pedestal, pointing to the apparent royal succession of Google over Microsoft and then Facebook over Google as evidence. This misses the point,

however, that there has been a decidedly new turn in the information economy that denies such a simplistic linear reading of history and innovation. This new turn concerns the emergence of multi-sided markets, an economic formation that is illustrated by examples as diverse as credit cards companies (Visa etc.) or even dating websites. In a multi-sided market, the task of the successful business is to bring together two or more distinct groups and then profit from the extraction fees charged as a result of bringing them together. For many Internet-based companies, this plays out in no longer having to innovate themselves. Instead they build a platform that brings together apps and users – as pioneered in the pre-Internet computing realm by Microsoft and IBM. The entire point of a platform here is a deviation from the traditional open-source story, only with a proprietary layer of profit extraction added in that it is far easier to 'outsource' the creation of applications than to build them in house, thus in effect creating a unified yet controlled platform on which others can invent. It is therefore useful to distinguish between invention and innovation in technical systems such as the Internet and Web. The Internet and Web have intrinsic architectures defined by their standards that offer themselves as a series of constraints such that 'the choice of possibilities in which invention consists is made in a particular space and particular time according to the play of these constants', - although ultimately innovation lies in the ability to give these choices technical flesh so that they can interact with the wider world; 'the rules of innovation are those of socialization' (Stiegler, 1998: 25-26). Any application developer can be ruined if they attempt to leave a platform and its captured market of users, as exemplified by the fall of the once-powerful corporation Zynga, who created the popular Farmville application for Facebook, as soon as the social networking site decided to end their 'special' relationship. The immense power of the platform thus becomes apparent: Facebook controls the socialization of applications, but more importantly the socialization of users – the very life-activity of their users on the Internet.

On the Internet, for a platform to be complete it must be composed of the hardware, the software, and the channels that are used for social co-ordination in order to harness the distributed problem-solving capacities that characterize collective intelligence. Thus, the platform is founded on the control of online social life on all levels. The Internet is likely to continue to be the transport protocol of choice in most if not all platforms due to its resiliency and widespread deployment – attempts to control the protocol layer by single corporations like Microsoft have at this point been mostly cast

off as failures – but all key software and hardware harnessed by the user must be under control. In order to fully extract value from the social co-ordination of its users, the technical platform has to watch over its users like a good shepherd, from the moment the user wakes up to the moment the user falls asleep ... and now there are even applications to monitor sleep patterns.

In this respect, the primary example of a platform is Apple, as it controls the hardware production of the iPhone, the core operating system that all applications use, a Web browser Safari, and data-services such as iTunes and iCloud that host the user's data. Thus, a user wakes up into a virtual company town consisting entirely of Apple products: they wake in the morning with a buzzer from their iPhone, listen to Music via iTunes, and communicate via Apple Mail and iPhone apps. Different vendors have different strengths, but it is the goal of every platform vendor to capture all aspects of online life. Any platform that does not absolutely control a service that features prominently in everyday life is at risk of failing: Microsoft is willing to spend huge amounts of money to create their own alternative search engine Bing to counter Google's heavy advantage in terms of possessing the world's preeminent search engine, while Google must do everything it can to undermine Microsoft's advantages when it comes to operating systems and office software by producing its own rival versions in the form of Android and Google Docs. Firms that fail to develop into their own full-featured, multi-sided market platforms are at risk of being cut out of the market altogether by one of the major platforms. It is a trivial matter for a platform to redirect a user's activity to parallel services that are run by the same firm that controls that part of a platform the user needs to access 'higher-level' services (although it is often technically illegal, as various antitrust verdicts in courts have shown).

Platforms that are missing critical components will either be forced to make alliances with other platforms that threaten their key advantages, such as the strange relationship between Facebook and Microsoft, or create their own missing components, like Amazon's attempted quixotic 'Axis' browser and the persistent rumors of a Facebook smartphone. This control of online life comes with tremendous power, like the control of life in the most general case that becomes increasingly inseparable from online life. A platform can charge inventors – application developers in particular – a high cost for accessing their users: an extraction of rent. The parallel extends further, as users are effectively cognitive serfs in these new immaterial feudal arrangements. The platform controls not only the

socialization of invention, but the socialization of users, as their ability to communicate can be limited to others on the same platform (Facebook), or serve as a source of value creation through data-mining (Gmail). Perhaps even more chilling, their very memories in the form of documents, photos, and videos are owned by the platform. One can only imagine the tremendous value, and what possible chunks of flesh, could be extracted if a platform wanted to charge for access to the externalized memories of their users. Yet unlike the content industries, the truly intelligent platforms have given up on this strategy of owning content, as its far better to do as Google does and enable users to create content for the platform for free – or, more accurately, for the privilege of accessing the platform for free. The good shepherd of the proprietary platform harvests their users as sheep, first for their fleece and then for their very lives.

Given the constraints of the platform the Web becomes increasingly crucial, since as HTML editor Ian Hickson points out: 'The Web's technology stack is ... the only platform that is completely vendor-neutral and not centrally developed. Anyone can invent a new feature and if the market agrees, can get that feature to be a de facto part of the platform' (Lawson, 2013). The Web's unique status in this respect was the result of a political battle between Tim Berners-Lee, the inventor of the Web, and the various browser vendors such as Microsoft and Netscape who were intent on fracturing the Web into HTML that was 'best viewed with Netscape Navigator' or 'Microsoft Internet Explorer'. Rather than attempting to create an alternative platform that would be free of the influence of proprietary firms, Berners-Lee used his role as lead author of the specifications that defined the Web to create a consortium that convened the Internet companies, and so started the second oldest of organization of the immaterial aristocracy: the World Wide Web Consortium (W3C). Unlike the anarchic IETF, the W3C is composed of organizations, primarily companies that come together in various Working Groups to create, via industry consensus, W3C Recommendations. These Recommendations (again, officially 'recommendations' as they have no nation-state standing, although they do adhere to a strict intellectual property agreement) are an evolving group of standards that define the Web as a universal and platform-neutral space of information. Sensitive to the issue that the immaterial aristocracy could be corrupted by undue corporate influence over a standard-making process where all work is done voluntarily (but often by professional standards experts), the W3C has its own independent staff to keep the process neutral and

preserve the core architectural values of the Web. Although technically a membership organization, the W3C does its work in the public and, up until the 'last call' for standardization, all comments from the public must be responded to, while members of the public who demonstrate expertise in the field can be let into the standardization process by W3C staff. Using this methodology, the W3C was able to create a version of HTML that worked across all browsers. While eventually Netscape was undermined by Microsoft in their nascent effort to create a platform that included the Internet, the ability of HTML to be vendor-neutral allowed for the creation of Mozilla Firefox and eventually enabled the rise of Google Chrome, which may likely become the next hegemonic platform. Still, the Web today is currently fractured between multiple platforms, with the W3C maintaining a very delicate peace between the various vendors, improving HTML (HTML5) and adding new capabilities such as Web cryptography.

However, a failure on the part of the W3C has led to the Web serving as both a platform for the universal sharing of knowledge and for universal surveillance. In Berners-Lee's original design, all users of the Web were to be treated equally and all data was to be shared for free, in keeping with the architecture of the Internet. Yet in order to keep 'state' on a user (similar to how deep packet inspection keeps 'state' on a packet), Netscape introduced a tiny, simple piece of code that could stay in a browser and relay information back to its owner about a user. Initially used to customize webpages and a crucial part of 'logging in' to websites, cookies are now tracking every click and visit of users across the Web. The capture, use, and selling of this data is now the de-facto business model of the Web, as such personal data is invaluable to marketers in the placement of what are known as 'behavioral' advertisements: ads that are targeted to a user's behavior. Due to constant improvements in machine-learning regarding this data, it can feel uncanny to users when the Web seems to know the content of their private messages and can recommend products and services to them accordingly, based on the most intimate of details. Due to government threats to regulate this practice from both the EC and USA, the W3C convened a Working Group to create a standard 'Do Not Track' (similar to 'Do Not Call' in direct marketing directors) that would let a user opt-out of being tracked by third-party cookies. However, the standard-in-making collapsed due to an argument reminiscent of a theological debate in medieval times (and remember that such arcane Christian debates were often the cause of very real conflicts during this period of history). This concerned the issue of whether users should or should

not be tracked by default. In one of the most brutal attacks in the platform wars, Apple and Microsoft had their browser turn off tracking by default. While they may claim to have done this on behalf of users, the real reason for their doing so was because it hurt Google's profit margins. Mozilla, which many idealistic open source advocates might assume would want to defend user's rights to privacy, actually survives primarily via payment from Google, and so it supports Google's interpretation of the matter. When entire platform business models are on the line, the peace treaty of the immaterial aristocrats is torn to shreds.

This is only the beginning, of course: there is even more valuable marketing data kept as people's 'private' personal data on social networking sites such as Twitter and Facebook. This data currently exists in an unregulated and unstandardized legal limbo. Attempts by various factions of the immaterial aristocracy at the W3C and IETF to standardize personal data have all been rebuffed, despite the noble goals of giving users the freedom to move from one platform to another ('data portability'), and even the ability to leave a particular platform ('the right to be forgotten'). Unlike some markets, once one is trapped in a platform, all technical forces conspire against escape. The European Commission has threatened to regulate such practices via the Data Protection Act, which embodies what can be thought of as 'the self determination of data' with a high respect for privacy. The fact that this ruling comes out of Germany is no historical accident: it is ingrained in the collective memory of Germany that the first step of the Holocaust was the collection of data about undesirables. Ironically, Facebook is now claiming to 'represent' their users against their own government and are lobbying against any data protection act – and in a 'vote' over privacy on Facebook, recently removed what little control users had over their privacy policy. The Data Protection Act may fail for an even more historically disturbing reason: various member-states have claimed a 'state of exception' to the regulation itself, as under the rubric of 'fighting terrorism' their police forces do not want to have to respect the right to privacy of data. As declining wages and mass unemployment make advertising-driven consumption less profitable, one market for personal data is the ability to control dissent. The same information that appears to enable corporations to innocently market consumer goods via behavioral advertisements, is a force as powerful as a 'nuclear weapon' when used 'against individuals by governments', according to Berners-Lee – especially given the fact that, under late capitalism, corporations and governments are often virtually indistinguishable, with the

United States being an exemplary case in point. In the words of Frank Rieger, privacy advocate and founder of the Chaos Computer Club : 'We lost the war' (Rieger, 2005)

As demonstrated by the successful struggle of users against SOPA, ACTA, and the WCIT, those platforms that are fighting for control of the net are no longer to be mediated purely by the engineering class of the immaterial aristocracy. On the contrary, the widespread penetration of the Internet has led ordinary users to both identify with the Internet in-and-of-itself, and to gain their own ability to self-organize. The slumbering giant of Internet users is awakening to its own potential force, and while these masses are currently focused primarily on net neutrality, all signs point to the possibility of an engagement in the defense of their rights to their own data. According to the old hacker's adage, one's data should have the same rights as one's own body. The immaterial aristocracy as an elite class of engineers may very well represent the transitionary figure on the stage of history, preparing the way for the arrival of users who can take social and technical responsibility for life online in their own hands. The greatest contribution of the immaterial aristocracy lies in their profound respect for the equality of access and the rights for data, which are ultimately ethical positions. The first step is to dive into what, in essence, distinguishes civil war from war-in-general, according to the anonymous French philosophical collective Tiqqun: that civil war is an ethical conflict between forms-of-life. Internet users must recognize themselves as a singular community with their own technological form of life, and with their own peculiar kind of ethics: 'The differences among forms-of-life are ethical differences' (Tiqqun, 2012: 50). The elaboration and politicization of these differences we have witnessed over the last year may ultimately lead to a true war between users and those who wish to control the collective intelligence of these users for the purposes of profit and domination. In the words of Amelia Andersdotter, the young Member of European Parliament from the Pirate Party, when confronted by those who wanted to enforce copyright on the Net: 'Fuck you, this is our culture'. Yet at this same moment various companies, such as Google, Microsoft, and Netflix, are using the W3C to attempt to force so-called digital rights management into HTML5, which would prevent video and other media from being easily copied and re-used if they embedded in an HTML web-page. Over the course of a single year, even the usually beneficent immaterial aristocrats of the W3C, who were once considered guardians of an Open Web, have come to be seen as inimical to the desires of ordinary users.

Conclusions

The immaterial aristocracy that has historically governed the Internet finds itself competing with traditional governments in the battle over WCIT and ACTA. Various companies whose business model depends on the free labour of Internet users present themselves as the champions of the Internet, and they did indeed successfully outmanoeuvre governments over the course of 2011 and 2012 with the help of an unprecedentedly large mobilization of ordinary Internet users. The final result of the last round of the immaterial civil war is that the traditional, heavily corporatist, immaterial aristocrats of the IETF and W3C have maintained their control over digital sovereignty against challengers like the ITU. Yet in 2013, thanks to issues such as the control of personal data and the division of the Internet into mutually incompatible proprietary platforms, it appears that the fragile alliance between Silicon Valley and ordinary users is fraying and may soon reach a breaking point.

Behind the immaterial aristocrats are the forces of Silicon Valley and thus global capital, a relationship that constrains the potential power of collective intelligence by binding it to short-term consumerism and the free production of content for proprietary platforms like Facebook – as opposed to allowing the collective intelligence of millions of Internet users to focus on global scale problems such as climate change that the market has spectacularly failed to solve. Indeed, in terms of social innovation, the potential power of collective intelligence lies unharnessed precisely because of its capture in proprietary platforms built by short-term capitalist logic. Of course, Silicon Valley views the Internet primarily as a source of profit extraction, but the digital natives who grew up with ubiquitous net access naturally view this technical infrastructure as part of their very lives.

If the Internet is truly a public space of shared intelligence with potentially vast distributed cognitive powers, then it seems it should naturally be a global commons governed by its users. However, the governance of such a global commons is today mediated by a very small set of actors, this being the immaterial aristocracy of bodies such as the IETF and W3C. Institutionally, both the IETF and W3C developed their structures in the 1970s and 1990s, before the great mass of digital native users were even born. As such, they operate as a mix of representative democracy and anarchic meritocracy, with decisions being made via fairly open multi-stakeholder processes. Yet, cognitively, such processes usually involve only dozens or at

most hundreds of individuals. However, if the Internet is now truly to be a global commons for collective intelligence, its governance must involves million and stretches across traditional governmental boundaries. How can the immaterial aristocracy become a true immaterial democracy that can do justice to the importance of the Internet? If it fails, will there soon be another round of immaterial civil war that pits the platforms controlled by Google and Facebook against their own users. One end-game is that the Internet will simply end up being consumed by a single victorious platform, such as Google. Another is that users will somehow band together and establish their own methods of governance, and use their potential power within these platforms to disturb value extraction, much as the traditional unions were formed by workers for the large corporations that dominated the industrial revolution, and who soon learned the power of the industrial strike.

The importance of the Internet should not be under-estimated, and a turn back to Marx can be helpful in illuminating the ramifications of immaterial civil war through another lens. That said, there are far more questions here than answers. Obviously, if Internet platforms gain their power via the control of the social life of users, how does this differ from the way in which traditional factories harness the power of workers, and can various theories of real subsumption account for the power of these new platforms? There is a need for a real inquiry that can locate the more utopian visions of theorists such as Hardt and Negri in the power dynamics of Silicon Valley, and a more grounded technical context (Hardt & Negri, 2001). After all, there has been no Internet-driven transition to communism as the various theorists of post-autonomism desired, albeit somewhat vaguely. Instead, there has been a financial crisis and massive social confusion with no clear signs of a political force emerging that can address the situation. Given the stunningly predictable crisis of capital we are currently in the midst of – if nothing else, Marx was correct about the cyclical nature of capitalist crisis – Negri, Badiou, and a whole host of contemporary philosophers have intuitively grasped that a new political force is needed to jump on the historical stage. Yet they commit the most elementary of errors by attaching such a force to the blood-stained historical failure of communism, a problem 'in which not to use the word is inevitably to fail politically, while to use the word is to preclude success in advance' (Jameson, 2009: 12).

Let us then name the unnameable political force that potentially stands against the dying (neo)liberal ontology of the profit-seeking

and consumerist individual: collective intelligence. From this point of view, the Web and the Internet are merely the technical underpinnings that allow this collective intelligence to flourish. However, just as the traditional workers movement existed before being fully theorized, and even dubiously reaching self-consciousness via the form of the party, the new forces arising on the Internet also lack self-consciousness of their situation, much less a well-developed strategy and an adequate organizational form. And like the traditional workers movements which featured their own cultural forms of songs and union halls, the digital natives are now developing their own unique cultural forms, too, from cat memes to Anonymous. The stretching of their collective muscles in the immaterial civil war with regard to ACTA and WCIT show that the digital natives do indeed have political power. The next battle in this war, that over personal data, will determine if they may even have the ability to wield this power against the corporate platforms that currently harness their collective intelligence in the search for profits rather than the wide-scale social innovation necessary in a world of ecological crisis and ever-increasing unemployment.

All politics is grounded in ethics, and ethics is grounded in ontology. For digital natives, the collective intelligence of the Web is part of their extended mind and the data they produce part of their extended body, all of which amounts to a very different ontological view from that based on a strict separation between the individual and the world. The full political ramifications of this ethical understanding of digital technology are just being felt in the larger world. Thus, there is more at stake in the immaterial civil war than the mere transition of power over digital sovereignty. When one speaks about defending the Web, one speaks of more than servers and software; the Web-as-technology is a stand-in term for the densely intertwined techno-ecological fabric of the world as created by late capitalism. This subtle mixing of metaphors reveals the crucial ethical content at the heart of everything from Anonymous to the Pirate Party, along with a profound ethical difference between not only pre-Internet forms of governance and digital natives, but between Silicon Valley and digital natives. When one no longer sees individuals as separate from technology, or technology as separate from nature, one glimpses the immanent totality of the web, a totality that stretches beyond the values of consumerism and profit-maximization promoted by global capitalism. The power of the Internet and the Web is that they are a mere technical infrastructure that is more amendable to our present-day cognitive grasp than the totality of existence, and this lets the World Wide Web be a

compelling cognitive stand-in for a totality that also contains within it webs of other kinds, ranging from food webs that connect solar energy, to human metabolism, as well as capitalist webs of production, distribution, and consumption. Dimly grasped by cognitive psychology and vague talk of post-humanism, this shift between viewing individuals as separate from their wider world to their being fundamentally, ethically and ontologically constituted by their wider social and technical worlds, although small, nonetheless carries the weight of a whole new world that is dying to be born.

References

Binstock, A. (2012) 'Interview with Alan Kay', *Dr Dobb's Journal* (July 10): http://www.drdobbs.com/architecture-and-design/interview-with-alan-kay/240003442

Carpenter, B. (1996) 'Architectural Principles of the Internet,' *IETF RFC 1958*: http://www.ietf.org/rfc/rfc1958.txt.

Galloway, A. (2009) 'Debord's Nostalgic Algorithm', *Culture Machine* 10: http://culturemachine.net/index.php/cm/article/view/350/352.

Halpin, H. (2008) 'The Immaterial Aristocracy of the Internet', *Mute* (2) No. 8: http://www.metamute.org/editorial/articles/immaterial-aristocracy-internet

Halpin, H. (2013) 'Becoming Digital: Reconciling Theories of Digital Representation and Embodiment', *Philosophy and Theory of Artificial Intelligence: Studies in Applied Philosophy, Epistemology and Rational Ethics*, *Volume 5*: 199-213.Hutchins, E. (1995) *Cognition in the Wild.* Cambridge: MIT Press.

Jameson, F. (2009) 'Three Names of the Dialectic', *Valences of the Dialectic*. London and New York: Verso.

Lawon, B. (2013) 'Interview with Ian Hickson, HTML editor'. *HTML5 Doctor* (January 8): http://html5doctor.com/interview-with-ian-hickson-html-editor.

Leiner, B. *et al.* (2003) 'Brief History of the Internet', *Internet Society*: http://www.isoc.org/internet/history/brief.shtml.

Maturana, H., and Varela, F. (1973) *Autopoiesis and Cognition: The Realization of the Living.* Dordecht: D. Reidel Publishing.

Negri, A. and Hardt, M. (2001) *Empire.* Cambridge, Mass: Harvard University Press.

Protalinski, E. (2012) 'Richard Clarke: China has Hacked Every Major US Company@, *ZDNet* (March 27): http://www.zdnet.com/blog/security/richard-clarke-china-has-hacked-every-major-us-company/11125.

Rieger, F. (2005) *We Lost the War, Welcome to the World of Tomorrow*: http://frank.geekheim.de/?page_id=128.

Madrigal, A. C. (2012) 'Bruce Sterling on Why It Stopped Making Sense to Talk About "The Internet" in 2012' *The Atlantic* (December 2012): http://www.theatlantic.com/technology/archive/2012/12/bruce-sterling-on-why-it-stopped-making-sense-to-talk-about-the-internet-in-2012

Stiegler, B. (1998) *Technics and Time, Volume 1.* Trans. R. Beardsworth & G. Collins. Stanford: Stanford University Press.

Tiqqun (2012) *Theory of Civil War*. Trans. Jason Smith and Alexander Galloway. Boston: MIT Press.

Zittrain, J. (2008) *The Future of the Internet and How to Stop It*. New Haven: Yale University Press.