2009

Introduction: New media and the reconfiguration of power in global politics

Athina Karatzogianni, Dr, *University of Hull*

[this is the manuscript pre-publication]

1. Introduction: New media and the reconfiguration of power in global politics

Athina Karatzogianni

Neo-liberal governments and institutions face a counter-hegemonic account of globalization, to which they have responded in a confused and often contradictory manner. One of the interesting sides to the argument is that the information revolution is altering the nature of conflict by strengthening network forms of organization over hierarchical forms. In contrast to the closure of space, the violence and identity divide found in ethnoreligious discourses, sociopolitical movements seem to rely more on networking and rhizomatic structures. US power is increasingly faced with resistance movements operating on a network model and utilising new information technologies.

These movements can be divided into two broad groups, ethnoreligious movements and sociopolitical movements. (Of course, there are cultural and life-style activism, movements but I would not make it my concern here). To suppress both kinds of movements, the US state relies on a binary, repressive mode of identity-construction, which divides the world into 'them and us'. This approach is guaranteed to escalate rather than resolve conflict. Its effects include the corrosion of civil and human rights and, most importantly, the increasing isolation of the would-be power-holders amid a sea of swarming resistances and uncontrollable spaces and flows. From 'with us or against us', domination therefore evolves into 'with or without you' (Karatzogianni and Robinson 2004; forthcoming 2009).

An example of the struggle to restrict and control the flow of anti-American propaganda is the effort by the U.S. Defence Department has blocked soldiers from accessing sites like YouTube and MySpace on its networks and their decision to

launch their own Multi-National Force-Iraq broadcasts. Having said that, the military personnel in Iraq has never been allowed access anyway. The ban really affects military personnel globally, which nevertheless can afford to access anyway through private service providers, use closed systems like Army Knowledge Online, or internet cafes, bypassing the ban from the DoD internet. What is ironic, but hardly surprising, is that this policy comes straight after a decision to create an official military do-it-your-self under the YouTube video-sharing mechanism. The logic is that if soldiers are blogging and vlogging, they should at least do it under military censorship and approval and channel their journalistic/cameramen ambitions in a controlled and filtered manner.

Channelling videos in a controlled manner is much more preferable for the military than having soldiers jeopardizing the multinational forces reputation, as has been the case in the past. It also produces an image of a military that is consistent with the current developments and embraces the technologies used by advanced countries and their citizens world wide. Yet, it remains doubtful that these videos will have an effect in the periphery of the world system, where people have yet to make a phone call. On a different issue, families of soldiers in Iraq and elsewhere are used to censorship. Regrettably, I think what will take some time to get used to is watching their loved ones fighting a war in online videos.

Nevertheless, this is part of an unprecedented operational tactic to counter the propaganda, organization, mobilization and recruiting techniques of Islamist extremist groups. The paramount example of this is Al-Qaeda's web presence and that of its affiliates. The Al-Qaeda network and its ideology relies more on common religious affiliation and kinship networks than strict national identity, which fits well with the borderless and network character of the internet. Significant is also the fact that the internet has been used as a primary mobilizational tool, especially after the breakdown of cells in Afghanistan, Saudi Arabia and Pakistan. On the internet, Al-Qaeda is replicating recruitment and training techniques and evading security services, because they cannot be physically intercepted, due to the virtuality of their networks. The internet is used by radical islamist groups under the ideological

umbrella global ‘ummah’ as a propaganda tool via electronic magazines, training manuals and general recruitment sites, as well as a weapon for financial disruptions aiming at financing operations, or stealing data and blueprints (see Dartnell ‘Web activism as an element of global security’, chapter 5, this volume).

Further, recognizing the medium and countering the enemy’s web presence is not the only reason for this current development in media policy. The past decade the US military has been consistently advised by think tanks to exploit new information technologies and create and sustain a more network-based approach to warfare, utilizing psychological and information warfare and ‘winning the hearts and minds of the population’. Especially post 9-11 and with the war in Afghanistan and Iraq, the US military has finally recognised the need to utilise new media and social networking technologies to tap into a younger American audience, recruit and mobilise global public opinion under a more favorable light of how this war is fought and why (on the question of public opinion and radicalization see Hoskins and O’loughlin, chapter 3, this volume).

Until very recently, the US military has been uncomfortable and clueless of how to deal with the uncontrollable and anarchic dimensions of the web, if efforts at cracking down on milbloggers and banning digital cameras following the Abu Ghraib scandal are anything to go by (see Touri ‘Transparency and accountability in the age of cyberpolitics: The role of blogs in framing conflict, chapter 4, this volume). The institution of embedded journalists and the crackdown of unilaterals in Iraq, ensured a patriotic media in the US, and elsewhere, however could not compensate for the increasing relevance of Al-Jazeera English, BBC world, and France 24, their online equivalents and ‘alternative’ media services and bloggers/vloggers (video) found in the web, indicating a transformation in the field of global communications due to the advent of the internet and its affiliated technologies (see Gardner, ‘War and the new Media Paradox’, chapter 2 this volume).

As the war continues, and domestic public support for the war decreases in the U.S., the military had no choice but to create a global outlet for its multinational force to bypass the global media which have become increasingly impatient of the war and more critical of its future. The YouTube videos of soldiers engaging with the local population, playing football with children and saving a kidnapped Iraqi is an effort to humanize an inhuman war. Nine out of ten top videos on You Tube are indeed military operations, 'a boots on the ground perspective'. What you see in these videos are soldiers that are simultaneously comfortable and uncomfortable fighting a war in front of a camera. It is a pornography of the simultaneous pride and suffering of these soldiers and the Iraqi population to an increasingly insensitivized audience.

The untilization of YouTube by the military raises important questions revolving around how information is released in the public domain and why, how much censorship is taking place and what alternative sources of information are available. These questions have to be posed in an analysis of the anti-Iraq war/pro-war, anti Islamic-pro-Islamic cyber conflicts we are witnessing today. The way a war is communicated is as important as the conduct of the war itself. Among many examples, the counter-propaganda YouTube effort by the Multinational Force-Iraq confirms that individuals and protagonists can now send stories more quickly than military press releases and mainstream journalists, indicating that civilian and military bloggers will have an independent capability to access future conflict arenas and to provide real-time visual and audio coverage of battlefield events. This has consequences for news management, even by very powerful states like the U.S.

In analyzing the March 2003 Iraq conflict, the internet's role in the conflict was studied, in terms of its effect on the organization and spread of the movement, and its impact on war coverage and war-related cyberconflicts. These last involved hacking between anti-war and pro-war hacktivists (sociopolitical cyberconflict), but also between pro-Islamic and anti-Islamic hackers (ethnoreligious cyber conflict) (Karatzogianni 2006).

On the sociopolitical cyber conflict field, the internet played a distinctive role in the spread of the peace movement, on war coverage and on war-related cyberconflicts, rendering the full potential of the new medium in politics and information undisputable. In the months preceding the actual war in Iraq, a plenitude of phenomena on and off the internet emerged, which in previous international conflicts were only embryonic. Before and during the war in Iraq, mobilization structures appear to have been greatly affected by the internet. Peace groups organized demonstrations and events through the internet, to the effect that 10 million people protested against the war globally, with the net speeding up mobilization remarkably. It helped mobilization in loose coalitions of small groups that organized very quickly, at the same time preserving the particularity of distinct groups in network forms of organization. Anti-war groups used email lists and websites, group text messages and chatrooms to organize protests, and in some cases, to engage in symbolic hacking against the opposite viewpoint. Accordingly, the anti-war movement succeeded in that respect at gradually building their own image of the Americans and their allies and framing their message (no WMD, dodgy dossiers, humanitarian concerns etc). The integration of the internet into mainstream media, the effect of online material challenging official government sources and the mainstream media, and blogging, are threatening the status quo countries and their representations in the global public sphere.

In terms of censorship, the latest literature supports the idea that journalists were not only censored and manipulated, but also targeted in this conflict—which brings up the issue of whether the U.S. could control information. Apparently, through psychological operations, they could manipulate the conflict and control the media, especially the American mainstream media (almost always submissive to the patriotic/nationalistic discourse after 9/11). However, the current change of US broadcasting in doubting the effectiveness of the administration's efforts, and the military's inability to control inconsistencies and fiascos from 24 hour internet coverage or to manipulate the American image in the Muslim world, has forced the military to reconsider its media tactics. All these developments are indication of where future conflict is going. The US military utilizes its younger generation of officers some of which are part of the internet generation, to reach audiences at home

and abroad in an effort to win the information war running parallel in cyberspace to the overly media manipulated conflict in the battleground.

One of the major differences between Vietnam and even the 1991 Gulf War, is that the internet has revolutionized not only coverage but has acted as a resource and weapon for the opposing parties in conflicts, a tool for organization, mobilization, and recruiting, even conflict resolution and hacktivism. In the 'first living room war', the Vietnam War, despite the fact that the network news deserve credit for the eventual disillusionment with the war, at the same time they were also responsible for creating, or at least reinforcing, the illusion of American omnipotence in the first place. An example of this was that American media delayed for two years the reporting of the My Lai massacre, not because of censorship, nor because the facts were not instantly available, but due to resistance to the story by the US media itself. That was because the massacre occurred in 1967, when the storyline was focused on 'good news' about a war which, editors were persuaded and the US was winning. There are some parallels to be found with the Gulf War war in 1991, however the major difference is that due to the speeds of 24 hour coverage and alternative reporting and blogging challenging the mainstream media in the online public sphere, the time the mainstream media waste on patriotism and disillusionment is remarkably decreased due to the checks and balances imposed by the internet revolution.

A further part of the cyberconflict environment is cyberterrorism: computer-based attacks intended to intimidate or coerce governments or societies in pursuit of goals that are political, religious or ideological. According to Arquilla and Ronfeldt (2001), conflicts increasingly revolve around knowledge and the use of soft power. This would come about with the help of information-age ideologies in which identities and loyalties shift from the nation-state to the transnational level of global civil society (see Egerton, chapter 8 this volume). Additionally, netwar is referred to as the low, societal type of struggle, while cyberwar refers more to the heavy information warfare type.

Cyberconflicts can act as a 'barometer' of real life conflicts and can reveal the natures and the conflicts of the participating groups. The protagonists in sociopolitical cyberconflicts fight for participation, power and democracy. Evident in the anti-globalization and the anti-capitalist movement is an alternative programme for the reform of society, asking for democracy and more participation from the 'underdogs', be they in the West or in the developing world. In the anti-war movement, which is a single-issue movement, the demand is for a change in power relations in favor of those that believed the war to be unjustified. In new social movements, networking through the internet links diverse communities such as labour, feminist, ecological, peace and anti-capitalist groups, with the aim of challenging public opinion and battling for media access and coverage. Groups are being brought together like a parallelogram of forces, following a swarm logic, indicating a web of horizontal solidarities to which power might be devolved or even dissolved. The internet encourages a version of the commons that is ungoverned and ungovernable, either by corporate interests or by leaders and parties (for a theorization of electronic civil disobedience see Meikle, chapter 12, this volume; for conflicts in netarchical capitalism see Bauwens, chapter 14, this volume).

Mobilization structures, for instance, are greatly affected by the internet, since the peace groups used the internet to organize demonstrations and events, to mobilize in loose coalitions of small groups that organize very quickly, and to preserve the particularity of distinct groups in network forms of organization. Moreover, the framing process was also affected, since email lists and websites are used to mobilize, changing the framing of the message to suit the new medium (see for instance Kavada's analysis of the organizing processes of the European Social Forum, chapter 13, this volume). The political opportunity structure in this particular case refers to alternative media, but also to an opening of political space, or an opening of global politics to people who, previously, would not or could not get as involved (for instance see Ganespachan's examination of web activism against gender violence, chapter 11, this volume).

Dissidents against governments are able to use a variety of internet-based techniques (email lists, email spamming, BBS, peer-to-peer and e-magazines) to spread alternative frames for events and a possible alternative online democratic public sphere. An example of dissidents' use of the internet is spamming e-magazines to an unprecedented number of people within China, a method which provides recipients with 'plausible deniability'. Also, proxy servers, file-trading networks like Kazaa and Gnutella can help dissidents communicate, since they have no central source and are hard to turn off.

Ethnoreligious cyberconflicts primarily include hacking enemy sites and creating sites for propaganda and mobilizational purposes. In ethnoreligious CC, despite the fact that patriotic hackers can network, there is a greater reliance on traditional ideas, such as protecting the nation or fatherland and attacking for nationalist reasons. The 'Other' is portrayed as the enemy, through very closed, old and primordialist ideas of belonging to an imagined community (for the impact on the Sri Lankan conflict see Vidanage, chapter 10, this volume).

The Israeli-Palestinian cyberconflict saw the use of national symbols (like the Israeli flag, Hebrew text and even a recording of the Israeli national anthem) when hacking the Hezbollah home page. This explicitly draws attention to issues of national identity, nationalism and ethnicity. Also, the language used by hackers relies on an 'us' and 'them' mentality, where Israelis and their American supporters, or else Palestinians and Muslims, are portrayed as barbaric, reflecting discourses of inclusion and exclusion. The internet in this cyberconflict became a battleground and was used as a weapon by both sides, and full-scale action by thousands of Israeli and Palestinian youngsters involved both racist emails and circulating of instructions on how to crush the enemy's websites. Similarly, in the Indian-Pakistani cyberconflict, the Indian army's website was set up as a propaganda tool, and hacked pictures of alleged tortures of Kashmiris by Indians were placed on the site, in a similar propaganda tactic. Also, the internet was used as a weapon, when the worm Yaha was released by Indian hackers. In particular disourses, religion is mentioned (religious affiliation), the word 'brothers' (collective identity and solidarity), and 'our country',

a promised land (Karatzogianni, 2006; see also here Rawnsley's analysis of the Taiwan Strait cyber conflict chapter 2 this volume).

The more recent Estonian cyber conflict is by no means then the first cyber conflict. We have been witnessing conflict in computer-mediated environments, as early as 1994. The reason the Estonian case has been coined the 'first cyberconflict or cyberwar' is because a nation's infrastructure was targeted in its entirety, in an orchestrated, unprecedented and sustained manner. The attackers used a giant network of bots as many as one million computers in places as far away as the United States Peru, China, Vietnam to amplify the impact of their assault. In a sign of their financial resources, there is evidence that they rented time on other so-called botnets.

The scale of the Estonian cyber conflict points to the deficiency of the international community to regulate cyberconflict, to create mechanisms for defining and then reacting to cyberattacks on a state, especially one linked to NATO and the EU, in a sensitive geopolitical area (for regulation issues see Delibasis, chapter 5, this volume). Despite the magnitude of a monthly assault on a country nicknamed e-Stonia, due to its reliance on online services, and the home of internet pioneers, Nato sends experts to learn from it, refraining from directly addressing the allegations made by the Estonian government or challenging Russia's stand.

Keeping the socio-economic implications in mind, the real impact of the Estonian cyberconflict operates on multiple political levels. First, whether the attacks where by the Russian government, Russian diasporic communities, or more likely Ethnic Russians in Estonia, the fact remains that NATO does not yet define electronic attacks as military action even if the guilty party is identified. Secondly, information communication technologies are a very convenient and cost-effective tool for protest, but the real spark are the uncertainty about the enemy within and the anxiety about the always incomplete project of national purity so that 'these geographies are the spatial outcome of complex interactions between faraway events and proximate fears, between old histories and new provocations, between rewritten borders and unwritten

orders', as Appadurai (2006) puts it. This cultural struggle, which integrates war and politics at the borders with vigilance and purification at the centers, is exarcebated by the media in general and by new communication technologies in particular. The fight to win the global war of messages, propaganda and ideas has often produced unpredictable results, especially in cyberspace. In essence, they are then defending the purity of their national space, and they do so by skilfully using online media technologies. To put it simply, globalization and its technologies can expose pathologies in the sacred ideologies of nationhood (for a discussion on small, virtual states and minorities online representations Karatzogianni, chapter 9, this volume).

As today's ethnic groups number in the hundreds and thousands, their mixtures, cultural style and media representations 'create profound doubts about who exactly are among the 'we' and who are among the "they" in the context of rapid migration or refugee movements, how many of "them are now among us" (Appadurai 2006). The statue and its removal in Estonia, and the cyberconflict that ensued is a reflection of the instability of the EU enlargement project, especially in relation to Russia's hegemonic aspirations, energy disputes and legacy in the region, pointing to an emerging second Cold asymmetric warfare by Russia, such as the recent missiles dispute with the US and Russia's relentless involvement in the region as a whole (supporting secessionist states, intervening in coloured revolutions, embargoing products etc).

In the final analysis, the true bigger picture must include a recognition that Russia is an Oligopoly (some even goes as far as to say a dictatorship cracking down on civil liberties), not to say that the U.S. is the paragon of democracy, holding together through the illusion of still providing a counter voice to US imperialism. As the US has a lot currently on its plate, any future action in defense of Nato countries in the former Soviet sphere of influence will destabilize consensus on the war on terror. Ultimately, a serious consideration, regulation and prevention of cyber conflict and its future implications might indeed require a bigger electronic Pearl Harbor than that of the Estonian cyberconflict.

It seems that the accusations against the Chinese attempting cyber espionage might be a turning point of how seriously governments take cyber conflicts and their regulation. The Chinese government has denied that the Chinese military is to blame for the cyberattacks involving systematic network penetrations against the US, Britain, Germany, France, and New Zealand, also pointing that such accusations are irresponsible and have ulterior motives. They are arguing that they have long opposed cybercrime and have explicit law and regulations against that and China 'does not do such despicable things'. German Chancellor Angela Merkel, after her own office and several government ministries were found to be infected with spyware, brought up the issue directly during her visit in China, warning that the two countries should observe 'a set of game rules'. The response by the Chinese government was to distance themselves from the accusation while promising to cooperate with international efforts to combat cybercrime.

Although the Chinese government is rounded and blamed by most experts in the field for these attacks, the countries attacked in most cases avoid directly accusing the Chinese, and mostly 'raise the issue' with them or stress that they are not implying that they did it, like the French, hoping that the Chinese will control their military or they rogue citizens more effectively in the future or that they will not succeed in getting classified information next time.

Nevertheless, the reality of the situation is much more complex --interestingly a word used by President Bush to describe the American relationship with China-- as it points to problems in reporting instances of cyberconflict without hyberbole; combating with formal international regulations cybercrime, cyberterrorism, information warfare and industrial espionage; putting more strain to bilateral relations with China on a global level; pointing to serious doubts over the Chinese government's control of their own military; and threatening the country's image in the community of states just before the Beijing 2008 Olympics.

The cyberattacks can also be in the future an extra problem for diplomatic relations with China, side by side with intellectual property rights, freedom of expression, aggressive industrial growth and monetary policy, environmental concerns etc. China is currently feared by these powers. The reason is not plans for cyberattacks against navies, plenty of those lurking on the net and subsequently published years ago by military futurologists in China, where the information warfare field has produced all sorts of scenarios in par with the US. The Chinese information warfare theorists have been discussing this a long time now from a technologically inferior position arguing that information warfare can provide them with an asymmetrical advantage.

China is feared because it is growing at great speeds and is hungry for information, as is currently every other country in the world. Understandably, information on commercial, military technology and cutting edge industrial secrets is fierce. China is by no means the only country at it. Even if the compromised system is unclassified, combined information can produce good intelligence perhaps compromising industrial, military secrets and so on. For China to sustain its economic success, she must become a centre of innovation and technology, and she looks particularly keen to, that is why she is the main suspect.

When attacks happen, they normally either never become public or do become public years down the line. Governments refrain to tell the world that their systems are vulnerable. The US suffered attacks pointing to provinces in China since 2003 with Titan Rain, when systems at NASA and other networks (agencies in Arizona, Virginia, San Diego, Alabama) were attacked retrieving information on aviation specifications and flight-planning software. This became public only in 2005. Therefore, it is especially curious that the attacks this June came out as quickly as they did. Reactions of the countries under attack will vary, as there is no regulation over information warfare on an international level. There is not even international cooperation on the issue of ICANN and internet governance, despite efforts at a world summit, let alone against cyberterrorism. For example, as pointed out by American officials, tracing hackers who use Chinese networks is complicated by the lack of cyber investigation agreements between China and the United States.

Generally, response varies from counter-attacks, for example such as the one reported by the Times during Titan Rain when US security expert Shawn Carpenter counter-hacked the intruders to the restrained recent reaction of the Prime Minister of New Zealand Helen Clark, who says she knows which countries tried to hack into her government's computers but is refusing to name names commenting that 'that's not the way intelligence matters are handled'. Interestingly, she also said that it is something every country is experiencing.

The reaction of the US President George W Bush was that he was aware that 'a lot of our systems are vulnerable to cyber attack from a variety of places' and that he might bring the issue with the Chinese, which he never did, apparently confirming the role of his administration as a cheer leader to the 85 per cent of networks controlled by private business in his country. The UK's reaction is also interesting since alarm bells have been ringing for a long time by the countries experts, as the National Infrastructure Coordination Centre had warned of the attacks in 2005 and the scale as 'industrial'. Andrew MacKinlay, a Labour member of the Commons Foreign Affairs Committee, went on record as saying that the attacks came from China and accusing the government of covering up the scale of the problem and appeasing the Chinese.

Unfortunately, not every country has cyberlaws, and there is no law that deems cyberattacks as military attacks against a nation, so it seems that everyone is doing it now that there is no international regulation, and now they can get away with it. In the case of China, even if their military was involved and the Chinese government was turning a blind eye or was buying the data from independent hackers (although one has to be sceptical as the internet is controlled fiercely in China), who can be sure that other state or non-state actors did not disguise their attacks to come from China, since China was blamed anyway? British official Roger Cummings of the National Infrastructure Security Coordination Centre (NISCC) talks of 'countries' probing attacks against his country, while new Zealand talks of 'countries', and the US mentions attacks by state and non-state actors. The whole reaction of these countries feels like there is more to this than China.

Finally, there might be more to this than China and hackers, as it seems a particularly clumsy attempt to be orchestrated by senior state or military officials. Also, in China, as in everywhere else the field is scattered, information warfare specialists and hackers are not under a centralised command, and might not be easy to control their plans scenarios and attacks. What is for sure though, is that this revelation and the circus that followed it, has come just before the 17th Party Congress expected to be held in October in China, and just when the Chinese needed to look more friendly towards the West the most. Also, all this 'China-but-other-countries-we-cannot-name and non-state actors too', is confusing, and rounding up only China when she is doing so 'well' is somewhat suspicious.

Whatever the developments and transformations in the sphere of global politics, the new media technologies and the political opportunities they present are unsettling the world system, the are rendering it chaotic and they are having a deeper systemic effect than the more powerful actors care to admit. It remains to be seen whether information age ideologies, new modes of capitalism, conflict, activism, terrorism and war in cyberspace will ever transfer to the 'real world' reversing the opposite trend, and causing everyday effects on a bigger scale than we are witnessing today. Even so, we are undoubtedly living in interesting times and systemic uncertainty has always produced the most beautiful and monstrous changes in global affairs.

This volume explores, through theorization of contemporary empirical examples, some of these changes and cyber conflicts situated in the global political environment. Part I, *Transforming Media and Global Conflic*t, is dedicated to identifying, theorising and exploring the general problems and research questions emerging from the complex interaction of new media, ICTs, the internet, social networking, v/blogging, global conflict and its coverage. Part II, *Global Security and Information Warfare* discusses the challenges ICTs pose for global security, in regard to theorizing, regulating information warfare and explaining the use of technology by radical Islamist groups or groups in ethnic cyber conflicts. Part III, *Ethno/religio/cultural Cyber Conflicts*, explores empirical examples of new conflicts zones emerging, such as militant jihadism online, and the effects of vast virtual communications on gender violence, virtual states and small states' online representations, anxieties, and cybercultural environments. Part IV

Socio/politico/economic Cyber Conflicts explores the symbolic power, organization, communication of socio-political groups and the socio-economic conflicts linked to global capitalist practices, netarchical or otherwise.