Winter 2012

Cyberconflict and the Future of Warfare

Athina Karatzogianni, Dr, *University of Hull*

Cyberconflict and the Future of Warfare

Athina Karatzogianni

Introduction

Writing a brief history of cyberconflict of the last decade and speculating on the future of warfare is by no means an easy task. The reasons are plenty and it is worth mentioning a few here, as they do tend to get lost in colleagues' specialised debates in the fields of international relations and global politics, global and national security, internet security, new media political communication, international governance, internet governance, information warfare, critical security and the geopolitics of new technologies. Information communication technologies (ICTs) have unsettled in an unprecedented way the majority of academic fields, all of which are currently required to negotiate multi-level conflicts transferring from the real world to cyberspace or being created originally through cyberspace and spilling over to real life. Equally, as correctly pointed out by one of the reviewers of this chapter, this is a very fast-moving field. It is also a field, which is not solely dominated by states and traditional wars, but by movements, civil society organizations, protest events, insurgencies, network resistances, and ad hoc assemblages. These groups and their use of ICTs are the subject of this work, as these players are using social media technologies to punch above their weight, to challenge the supremacy of the state, as having the monopoly of violence and propaganda, through using ICTs as a weapon or as a tool for mobilization, organization and recruitment, and providing instant access to the global public sphere to influence the strategy, tactics and justification of wars, and resist the violent oppression of citizens by totalitarian and authoritarian regimes. The relevance of these actors and their use of technological innovation is currently more than critical with social media networking utilised to accelerate the regime changes in the Middle East region and elsewhere, and the military interventions the international community had to respond with due to the undeniable publicization of their plight in the virtual public sphere to protect the citizens of these states, point to the need to examine the history of the use of ICTs by these actors.

This global media transformation affecting international communcations has created theoretical and empirical problems reflecting the multi-disciplinary, interdisciplinary and cross-disciplinary character of cyberconflict,[1] and has resulted in a disparate literature, which only rarely comes together as one area of study.[2] In ontological, theoretical, and methodological terms, the claims and politics stemming from the various disciplines quite often clash, for instance information warfare, counterterrorism, cybersecurity and global communications studies are influenced by an inevitably conservative state and status quo bias with a positivist methodology resting on a realist and or neo-liberal politics, in direct contrast to more sociological, media and political theories resting on the centre or centre left of the spectrum, engaging with more qualitative methodologies and perhaps focusing on postmodern and poststructuralist explanations. Exceptions to this crude generalisation are evident all over the place, but it is indicative of the overall state of the literature in the last decade. An example of this amalgam of debates, academic areas and methodologies is this author's research monograph *The Politics of Cyberconflict* which theorises cyberconflict between 2000-2005 in terms of elements from three academic areas (media, social movement and conflict theories), looking at earlier ideas on information warfare and security and engaging with sociopolitical cyberconflicts (anti-globalization and anti-war movements, cyberdissidents and internet censorship) and ethnoreligious cyberconflicts (various examples such as Israeli-Palestinian, Indian-Pakistani spilling over into cyberspace), as well as the effect of the internet on the anti-war movement, coverage and cyberattacks.[3]

Since the publication of that work, a proliferation of linked subjects to cyberconflict has emerged. Even if it is impossible to encompass the diversity of issues here, it is worth mentioning briefly the kind of breadth one is faced with when discussing cyberconflict, in a way setting an agenda for future study:

The Individual and individual security in cyberspace (i.e. internet safety in vulnerable groups, for instance underage users)

Class, Gender, Minority, Migration issues, individuals and groups (i.e. the digital gap, digital have less, digital working class, digital diaspora networks and the digital development of migrants).

Private Corporations in the IT industry and elsewhere and their corporate, social and moral responsibility (ie. issues coming up in Google-China cyberconflict, issues of human rights, censorship, the cybersecurity professionals hawks vs. doves etc).

Civil Society – Non-state actors (i.e. the role of these actors in ensuring digital freedom, the methods used and the ethical debates and cybersecurity issues raised by NGOs etc)

The State – The role of the state and the difficulties of the boundry-less character of cyberspace, the inability of the state to embrace ICTs fast, adequately and if at all depending on its position in the global system (linked to that cyberconflicts in unrecognized and small states and cybersecurity effects in the struggle for statehood and survival). Also, questions of e-government as the last effort at state relevancy and survival.

International Relations – International Regulation- International Law regarding cyberspace (i.e. the problems related to the non-existence of these for situations such as Estonia, NATO, UN, EU, major INGOs, and serious problems in addressing violations and cyberattacks between states, see for example the China and Russia accusations made by Western governments over the last decade).

Global Politics, Political Economy – Wider implications for global politics beyond states, NGOs to include social movement organizations and their demonstrated overuse of ICTs, the transformations due to network forms of organization, mobilization and recruitment.

Media Convergence, Digital Economy Regulations -- Illegal file-sharing, fandom and purity brand control, transmedia marketing and story telling.

Global Media – The effect of the internet on media ownership, media coverage, for instance the Iraq war, security implications stemming from cybersecurity problems, radicalization media.

Global Resistances, Uprisings, Movements and their organization, mobilization, recruitment and ideological development/framing through cyberspace.

In this chapter, a brief summary of cyberconflict during the first half of the last decade will be provided, followed by a discussion of the major incidents of the second half of the decade, thereby engaging more broadly with the popularization of cyberconflict, cybercrime and cybersecurity as fields of enquiry in the media, government and private sectors. Moreover, the advent of Web 2.0 post-2005 creates unprecedented access to data and social networking witnesses a flourishing of flamewars, national homeland patriotic hacking, mobilization, governance, privacy, safety, piracy issues emerging, for example on Youtube, Facebook, Wikipedia and other platforms and virtual communities, which despite their empirical richness will not be part of our discussion here. Instead, the chapter after engaging with the most important empirical cyberconflicts and their linked subjects of the past decade, discusses theories of future warfare and future effects of war and conflict on politics, culture, media and society.

Cyberconflicts 2000-2005

Cyberconflict, defined as conflict in computer-mediated environments, has been witnessed as early as 1994 with the Zapatista guerilla movement in Mexico transferring their mobilization online and linking with the anti-globalization movement through the internet. In the late 1990s, Arquilla and Ronfeldt[4] expressed the idea that conflicts will increasingly revolve around knowledge and the use of soft power. Additionally, these Rand theorists defined netwar as the low, societal type of struggle, while cyberwar refers more to the heavy information warfare type. Here the focus is on the netwar type cyberconflicts, as historical incidents are explained and their implications for global politics and security are considered.

Cyberconflicts can act as a 'barometer' of real life conflicts and can reveal the natures and the conflicts of the participating groups. Before the advent of Web 2.0 two types of cyberconflict were prevalent: ethnoreligious (between ethnic or religious groups fighting in cyberspace) and sociopolitical (conflicts between a social movement and its antagonistic institution).

In sociopolitical cyberconflicts, such as the anti-globalization and the anti-capitalist movement, there is evident 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. New social movements are not new, but rather, part and parcel of the dominant modern culture, which makes it difficult to think of movements as flowing either from 'pre-modern' or 'postmodern' subcultures. However, the structure of NSMs - open, decentralized, nonhierarchical - makes them ideal for internetted communication. The movement is composed of adverse autonomous units that expend an important part of their resources on internal solidarity. A network of communication and exchange keeps the cells in contact with each other. Information and resources circulate in networks, and leadership is not concentrated but diffuse. NSMs advocate direct democracy, self-help groups and cooperative styles of social organization. The fewer and weaker the social ties to alternative networks, the greater the structural availability for movement participation. Sociopolitical movements, such as the political dissidents in China, can test the limits of a system, pushing the system beyond the range of variations that it can tolerate without altering its structure.

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.

An early example of hacktivism (online activism) is the Seattle anti-WTO mobilization at the end of November 1999, which was the first to take full advantage of the alternative network offered by the internet. Also, dissidents against governments are able to use a variety of internet-based techniques to spread alternative frames for events and a possible alternative online democratic public sphere. Online efforts, such as pro-democracy, activist or anti-government websites point to the fact that people believe in the power of the medium enough to organize and run thousands of these sites. In many cases, they are able to initiate and control events, and mobilize and recruit others for their cause, as in the case of sites in the Islamic world, in China, in Latin America, activist sites for anti-globalization and single-issue protests and mobilizations both on national and international levels.

To continue, ethnoreligious cyberconflicts, primarily included hacking enemy sites and creating sites for propaganda and mobilizational purposes. In ethnoreligious cyberconflict, 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, which "patriotic" hackers will have to fight for in cyberspace.

For instance in 2001-3, the Israeli-Palestinian cyberconflict saw the use of national symbols, explicitly drawing attention to issues of national identity, nationalism and ethnicity. Also, the language used by hackers relies on an "us" and "them" mentality, where the internet 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 was used as a weapon, and in particular discourses, religion is mentioned (religious affiliation), the word "brothers" (collective identity and solidarity) and "our country", a promised land.

In contrast, 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. The internet has been used as a primary mobilizational tool, before 9/11, especially more 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 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.

In the March 2003 Iraq conflict, the internet's role was crucial in the conflict, on the organization and spread of the movement, 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 cyberconflict). Moreover, mobilization structures were 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. Furthermore, the framing process was affected as well, since email lists and websites were used to mobilize, changing the framing of the message to suit the new medium. The language used to mobilize through the internet differs from traditional political discourse (for instance, speeches or texts in traditional media) in that it can combine various technical media (video, satellite images, file-sharing) in a way that delivers on the one hand a richer message, but on the downside a sometimes hasty and crude, under-analytical political message. The political opportunity structure in this particular case can refer to the rise of alternative media, but also to an opening of political space, and an opening of global politics to people who would not or could not get so involved before. In virtual terms, hacktivism was apparent in anti-war/pro-war hacking, for example a Virtual March on Washington, which impacted the city's communication infrastructure.

On the hacking front during the war Iraq, pro-Islamic/anti-Islamic hacking was an example of ethnoreligious cyberconflict. The link between ethnoreligious affiliation and discourses of exclusion/inclusion is evident, when considering the al-Jazeera hack from American hackers, and the movement of Islamic hackers united in a common anti-US, UK, Australia, anti-Indian and anti-Israeli agenda. Furthermore, the use of the internet as a propaganda and mobilizational tool was common to both sides in the sociopolitical side of it (anti- and pro-war), through a considerable amount of websites advocating one view or another and mobilizing, countermobilizing and anti-mobilizing against each other.

On the media front, it is clear that political discourse was constructed in the American mainstream media to mobilize support for the war, since, for example, more than two-thirds of all sources in news programs were pro-war. Also very important was the issue of alternative sources and censorship. Because of the embedded system, journalists having their work jeopardized for not being 'patriotic' enough, and the American media generally following the government line, Americans and the rest of the world went online to find alternative news and first-hand eyewitness accounts via emails and blogging and video logging. The result was the integration of the internet into media coverage and the distribution of online material challenging official sources. Anti-war groups had the ability to initiate and control protest events and to mobilize supporters, but were not as successful in dominating political discourse. The media effects on policy were, above all else, technical. As a result, there was instant 24-hour access to the war, bringing with it the pressure this would inevitably put on any administration. However, no actual debate or impact on policy took place, since the American media failed at least until 2005 to question any decisions being taken by their government.

In the final analysis, the internet played a distinctive role in the spread of the peace movement, on war coverage and on war-related cyberconflicts, in relation to which the full potential of the new medium in politics was shown. 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. 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. The integration of the internet into mainstream media, the effect of online material challenging official government sources and the mainstream media, and blogging, were indicative of future coverage, and where the first signs of what we are witnessing today.

Lastly, between 2000-05, there was a duality of cyberconflict, where ethnoreligious cyberconflicts were mapped as representing/defending loyalties of hierarchical apparatuses and sociopolitical cyberconflicts were empowering network forms of organization. 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.

Cyberconflict 2005-Present

Besides the acceleration of the use of the internet for radicalisation[5] purposes, by dissident and social movements around the globe,[6] the first serious incident of cyberconflict in International Relations terms at least, occurred in 2007 in Estonia.

The real life event that sparked the cyberconflict was the removal of a Soviet war hero statue from Tallinn's square caused riots in Estonia for a couple of days around the 26th of April 2007, which caused one death and several injuries. But by April 29, although the real-world riots calmed down, the country's digital infrastructure was crumbling from cyberattacks. The statue incident expressed the deeper tensions and the cultural conflict between the ethnic Russians in Estonia and the Estonian state, which makes up around one-quarter of the Baltic republic's population of 1.34 million. The country is considered to be a success story due to its e-commerce, which even sees government activities conducted on line.

In this cyberconflict we witnessed denial of service attacks, clogging the country's servers, routers, infiltrating the world with botnets, banding computers together and transforming them into 'zombies' hijacked by viruses to take part in such raids without their owners knowing. Multiple sources flowed into the system, the attackers even rented time in botnets. The attacks lasted 3 weeks. The plans of the attackers were posted in Russian language chatrooms with instructions on how to send disruptive messages, and which websites to target. The targets were on all social, political and economic levels: the Estonian presidency and its Parliament, almost all of the country's government ministries, political parties, three of the country's six big news organizations, two of the biggest banks; and firms specializing in communications. The effect was a rapid organization to fight the war from the Estonians utilizing contacts in several countries and asking NATO and the EU for help, blaming the Russian state for the attacks.

Although Estonia claimed the attacks originated in Russia, and the global press linked the attacks to the Russian government, it was eventually accepted that it was in fact nationalist hackers that had done most of the work. Members of Nashi, a private pro-Kremlin youth group, also claimed to have had a hand in launching attacks and state controlled media were reported to have helped whip up anti-Estonian fervor that may have helped recruit hackers. An ethnic Russian student, Dmitri Galushkevic, was convicted of attacks against the website of Estonian Prime Minister Andrus Ansip and would pay a fine of roughly 1100 Euros. The Estonian government, which complained that the attacks were orchestrated by Russia, were also portrayed as going through a panic attack, exaggerating the situation, when their networks were attacked in cyberspace.

Several issues emerged because of the attacks in Estonia. One of the main problems, was that NATO did not yet define electronic attacks as military action, therefore it cannot intervene even when the origin of attack can be proven. This issue has been a problem addressed by various authors.[7] What is more interesting is that in June 2010 it was reported in the *Sunday Times*[8] that a team of NATO experts led by former U.S. Secretary of State, Madeleine Albright, prepared a report among others saying that a cyber attack on the critical infrastructure of a NATO country could equate to an armed attack, justifying retaliation. The organization's lawyers were reported as saying that because the effect of a cyberattack can be similar to an armed assault, there is no need to redraft existing treaties. If an attack on critical infrastructure resulted in casualties and destruction comparable to a military attack, then the mutual defense clause, article 5 could be invoked. Still, the level of attack is not exactly clear.

Also, because of the Estonian incident, the role of information communication technologies was yet again explored as a very convenient and cost-effective tool for protest – usually related to hacktivism and the ethical debates involved. Linked to the real life protests and their online incarnation is the real spark are the uncertainty about the enemy within and the anxiety about the always incomplete project of national purity reflected in the ethnic Russians leaving in Estonia and elsewhere. These cultural struggles are exacerbated by the media and propaganda, with groups defending the purity of their national space using online technologies. The Estonian cyberconflict is also a reflection of the instability of the EU/NATO enlargement project, especially in relation to Russia's hegemonic aspirations, energy disputes and legacy in the region, with Western reports pointing to an emerging second Cold asymmetric warfare by Russia, such as the missiles dispute with the US and

Russia's relentless involvement in the region as a whole (supporting secessionist states, intervening in 'colored' revolutions, embargoing products etc).

Another major incident was in the case of Georgia, however the circumstances were different. It was reported as a "virtual war" in cyberspace accompanying the brief actual war in the summer of 2008 between Georgia and Russia. Again Russia was accused of orchestrating the cyberattacks and again it turned out that although coordination with the military was not deemed impossible, it was largely due to patriotic hacking.

Russia sees armament in Georgia as a serious problem and it has brought it up in NATO meetings after the war at meeting in Brussels. In December 2009 NATO and Russia resumed their political dialogue, which NATO had broken off after the war in Georgia. All this discussion regarding global security espionage and cybersecurity is accompanied in the media with questions over NATO and Russia seeing the participation of former soviet influence countries as threatening. This is especially prevalent in the media debates when Estonia and Georgia cyberconflicts are covered, as well as NATO's cybersecurity capabilities, doctrine and general regulation of cyberconflict.

The link of cybercrime to cyberconflict is explicit in reports that one of the botnets drafted for the Georgian cyberattack was Black Energy, a Trojan horse-hijacked army of PCs thought to have been used to hit Citibank, while Black Energy 2 was being used to launch DDoS attacks against Russian banks. Political and patriotic hacking is not only linked to cybercrime, but to the Russian intelligence service, the FSB, in the Georgian press.

In November 2009, Russian hackers and Russia were immediately implicated in the Climategate hack, when emails exchanged between key climate change scientists of the Climate Research Unit at the University of East Anglia were posted on a Siberian server, creating a debate over peer review and the climate change debate when the Climate summit in Copenhagen was occurring. The Russians were portrayed in a Cold-War propaganda discourse in the media as having the motive to want to discredit the summit, poor talented unemployed Russian hackers would have been easy to employ, while the use of patriotic hackers by the Russian secret service the FSB fitted the narrative. Although there is no resolution on who was responsible for the hack, it seems that the Russian connection definitely is not as strong as in the original reports, with analysts even talking about computer security failures at the university involved to have been more likely coupled with the likelihood of American climate skeptic bloggers having played a role at least in the dissemination of the files.

A few months later, in January 2010, one of the most complex cyberconflicts occurred, when Google reported the attacks which took place towards the end of 2009 as originating in China, penetrating their network to steal intellectual property (source code) and hacking into gmail accounts held by human rights activists, with a declaration on changes in their China policy. Revelations were made about similar attacks involving more than thirty companies in a 2009 US-China Economic and Security review reporting to Congress a steep rise in attempts to infiltrate and disrupt US government sites from all over the world with China the largest single source.

The effects of this incident are wide-reaching in this field of research, as it brings together in one discussion, a complex matrix of debates. In the bigger picture, this cyberconflict event adds to the debate on the position of China in the world system, and creates insecurities about the ambitions, capabilities and hidden desires of the 'next hegemon',[9] while it punches more wholes to the odd Sino-American relationship. Further, it raises questions about China's information warfare philosophy and military doctrine and the bizarre and contradictory ways they develop their virtual society, i.e. exploiting the technologies commercially, but using surveillance and censorship in ways contradicting liberal ideal of universal digital rights. On top of these concerns are the transformations the internet has brought in regards to civil society, citizenship and activism;[10] the relationship between business and activism in China and beyond; the relationship between state and the plethora of 'patriotic' hackers; and the question of the working class digital have-less inside China.[11]

The result of the Estonia cyberconflict was the establishment by NATO of a Cooperative Cyber Defence Centre of Excellence (CCD COE or code name K5) in 2008 in Tallinn.[12] In May 2010, the secretary of Defense Robert Gates announced the activation of the Pentagon's first comprehensive, multi-service cyber operation, the U.S. Cyber Command (CYBERCOM), with Keith Alexander as its commander. Talking about cyberspace as the fifth battlespace, transferring soldiers from communications and electronics to an Army Forces cybercommand, and wondering on how should cyberwarriors should be trained, confirms a trend toward militarization what was previously criminal and commercial matters.[13] With Russia and China frequently the usual suspects, the U.S. and its NATO allies have had to address cyberwarfare questions in its 21st century strategic concept. With 120 countries developing cyber capabilities, NATO's Director of Policy Planning, Jamie Shea has commented that "there are people in the strategic community who say cyberattacks now will serve the same role in initiating hostilities as air campaigns played in the 20th century".[14] NATO will have to create a coherent strategy for cyberwarfare.

These historical incidents of cyberconflict of various types raise questions of cybersecurity, as a part of global security in global politics today. Unless the precise level, which makes a cyber attack part of armed conflict is defined by international law on cyberconflict, any cyber attack could be framed as cybercrime and prosecuted as such. This is turn would mean that any political hacking even for protest will be prosecuted as cybercrime. This could potentially mean that electronic disobedience or hacktivism as we have known it, despite having mostly symbolic effects can be also prosecuted under this logic. To this an added problem for global politics is the difficulty in understanding where attacks originate from and whether there are state-sponsored or ad hoc assemblages. Not having defined the level where a cyber attack becomes equivalent to an armed attack, there is no way currently to plan reaction on an international level. Furthermore, its is not clear whether cyberattacks and cyberespionage will be eventually considered as a kind of war, as information warfare and espionage historically have not be recognized as war or grounds for war.

Cyberconflict and Future Warfare

The most common view on information warfare and the future of conflict, whose best-known exponents are Heidi and Alvin Toffler,[15] extrapolates from the idea that territory, population and natural resources are becoming less important, relative to human capital and the possession of information. Taking this process to its logical conclusion, these theorists believe that information will soon become the key source of wealth and power – equivalent to steel, coal and oil in the industrial age, or fertile land in the agricultural age. This change will eventually amount to a social revolution, whose scope is equivalent to only two previous such transformations: the agricultural and industrial revolutions.

The transition will be from industry to information-based services and this will correlate with the "informatting" of warfare. Sun Zi is an icon in this pantheon, with his observation that the "acme of skill" consists in winning without fighting. Advanced technological systems will not only help shape the environment of future conflict, but will also magnify the importance of the psychological battle to the conflict outcome. At the systemic level, information warfare is the organization of information to provide warriors with what has been termed “dominant battlespace knowledge”. Insofar as the ability to kill what can be seen makes seeing (locating, identifying and tracking) the key to war, seeing is increasingly best done by networking sensors and human observers to create a shared foundational truth that forms the basis of command, control and operations.

Arquilla and Ronfeldt[16] argued at the dawn of the millennium that power seems to be migrating to non-state actors, who are able to organize into “sprawling multi-organizational networks”, which are more flexible and responsive than hierarchies in reacting to outside developments, and appear to be better than hierarchies at using information to improve decision-making. The battlespace of information warfare is cyberspace - an ethereal place which does not fit neatly into the land - sea - air space. Taking out all information-transfer media would bring down a country’s stock market, banking system, air traffic control, emergency dispatches and more. The rise of networks is likely to reshape terrorism in the Information Age and lead to the adoption of netwar - a kind of Information Age conflict that will be waged principally by non-state actors. The Rand corporation in the US also predicts that cyberterrorists will use new tactics such as “swarming”, which occurs when members of a terrorist group, spread over great distances, electronically converge on a target from multiple directions, a tactic different from the traditional form of attacking in waves, which delivers a knockout blow from a single direction on the internet.

Besides this type of argumentation on the future of conflict stemming from the counterterrorist literature in the U.S. and focusing on the Revolution in Military Affairs (RMA), there have been other contributions theorising war, media and culture more broadly, for example its relationship to postmodernity,[17] to culture and media as militainment, [18] and virtual war in general.[19] Hammond for instance explains that beyond the high-tech weaponry and the RMA discussion, war is becoming postmodern both in the sense of intra-state conflicts where we witness wars about identity politics, in the cosmopolitanism vs. exclusivism fashion, but also wars of humanitarian intervention, “spreading democracy”. Hammond argues that the West’s crisis of meaning after the end of the Cold War and the collapse of the grand narratives has caused a shift first to the therapeutic war (salvaging the reality of war in our own eyes - humanitarianism) to the War on Terror (Postmodern terror, as the west at war with itself, with Other regarding imperialism and nihilistic terrorism as products of the crisis of meaning). In Hammond’s explanation of postmodern politics, he cites Žižek’s argument that the elite takes over the language of the left: from identity politics to official multiculturalism as the ideal form of ideology of global capitalism, which does not disturb the circulation of capital. The idea of war as distraction is replaced by war used to engage a disengaged citizenry. The postmodern war becomes an exercise in risk management.

In this kind of logic Stahl[20] talks of the fusion of military and entertainment, as *militainment*: the transformation of war aesthetics from the 1991 Gulf war, where we consume a clean surgical sanitized war, a computer game technofetishism with the citizen spectator to Iraq 2003 were we have depictions of war as sports coverage, reality television, video games, with similarities to all these entertainment genres. Identity is absorbed into the military-entertainment matrix: A migration of identity to the interactive war. The spectator of 1991 becomes a virtual citizen-soldier, annihilating the viewer's capacity to distinguish between fact and fiction. This is similar to embodying the body in the military machine, like in the movie Iron Man: "An integrated machine of hardware and software interfacing the subject with the military apparatus".[21] As Stahl explains, conflict becomes a celebratory event, an exercise in recreational violence within a larger sea of fictitious violent entertainment.[22]

In turn, Der Derian in his *Virtuous War* argues that the global media is e-motive: a transient electronic affect conveyed at speed, where it is difficult to maintain the distinction between war and peace: "In this high tech rehearsal for war, one learns how to kill but not to take responsibility for it, one experiences 'death' but not the tragic consequences of it".[23] In this type of infowar, Der Derian tells us, they did not invent a new game: they made the virtuous war the only game worth playing.

Although it is impossible to predict the future of warfare, this chapter has attempted to show historically how cyberconflict, the role of networks, and communication technology infrastructures will be of paramount importance, not only in the way wars are fought, but also the way wars are communicated and justified to the global public. Not only that, but the acceleration of protest, due to the digital virtual enabling the grasping of political opportunity, when there is a crack in the global political structure by ad hoc assemblages, protest networks and other resistant movements, such as the situation with WikiLeaks and its effect on diplomacy, and spill over effects currently in the Middle East, points to the critical importance of political communication in the global transformations taking place all over the world. The move to overthrow repression, violence and fear through peaceful means and virtual protest and its real life materialisation of revolution seems to be perhaps rendering war an extraordinary response to be used only to protect and not maim life. The politics of justifying war beyond the protection of life will likely be debated for a long time to come, but the importance of ICTs as a factor in the political communication of future wars, protests and resistance is unquestionable.

Bibliography

Arquilla, John and Ronfeldt, David, (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, California: Rand, 2001.

Bronk, Christopher, "Webtrapping: Securing the internet to save us form transnational terror?", *First Monday*, 13, 11, 2008.

Central European University. Participants' reflections on workshop themes. "Cybersecurity: Europe and the Global Society Revisited: Developing a network of scholars and agenda for social science research on cybersecurity", 7-8 June 2010, Budapest Hungary, http://ww.cmcs.ceu.hu/cybersecurity/main

Dahlberg, Lincoln and Siapera, Eugenia, (eds.), *Radical Democracy and the Internet*, Basingstoke: Palgrave Macmillan, 2007.

Der Derian, James. *Virtuous War,* London and New York: Routledge. 2009.

Diebert, Ronald and Rohozinski, Rafal, "Risking Security: Policies and Paradoxes of Cyberspace Security", *International Political Sociology*, 1, 4, March 2010.

Dunn Cavelty, Myriam, and Mauer, Victor and Krishna-Hensel, Sai Felicia, (eds) *Power and Security in the Information Age: Investigating the role of state in cyberspace*, Ashgate, 2007.

Eriksson, Johan and Giacomello Giampero, "The Information Revolution, Security, and International Relations: (IR)relevant Theory?" *International Political Science Rview/Revue internationale de science pol.,* 27, 221-244, July 2006.

Hammond, Philip, *Media, War and Postmodernity*, London and New York: Routledge. 2009.

Hensen, Lene and Nissenbaum, Helen, "Digital Disaster, Cyber Security, and the Copenhagen School", *International Studies Quarterly,* 53, 4, 115-1175, 2009.

Johnson, Bobbie. "No one is ready for this", *The Guardian*, April 16, 2009, http://www.guardian.co.uk/technology/2009/apr/16/internet-hacking-cyber-war-nato

Karatzogianni, Athina. “Blame it on the Russians: Tracking the Portrayal of Russians During Cyber conflict Incidents”, *Digital Icons: Studies in Russian, Eurasian and Central European Studies,* Issue 4, November 2010.

Online available at: http://www.digitalicons.org/issue04/athina-karatzogianni/

------“The thorny triangle: Cyber conflict, business and the Sino-American relationship in the global system”. *E-International Relations*. 10 March 2010, http://www.e-ir.info/?p=3420.

------(ed.) *Cyber Conflict and Global Politics*, London: New York Routledge. 2009a.

----“Confronting internal and external problems of cross- inter- and multi-disciplinarity: researching cyber conflict and global politics” in Karanika, M and Wiesemans, R (eds) *Exploring Avenues to Cross-Disciplinary Research*, Nottingham University Press, 2009b.

------*The Politics of Cyberconflict*, London and New York: Routledge, 2006.

Karatzogianni, Athina and Michaelides, George. “Cyberconflict at the Edge of Chaos: Cryptohierarchies and self-organization in the open source” in Phoebe Moore and Athina Karatzogianni (eds.) *Parallel Visions of P2P production: Governance, Organization and the New Economies,* Special issue*, Capital and Class*, 143-159 January 2009.

Karatzogianni, Athina Karatzogianni and Robinson, Andrew, *Power, Resistance and Conflict in the Contemporary World*, Routledge Advanced Series in International Relations and Global Politics, Routledge: London: New York, 2010.

Liaropoulos, Andrew, “War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory”, Proceedings of the 9th European Conference on Information Warfare and Security, University of Macedonia, Thessaloniki, Greece, 1-2 July 2010.

McCaughey, Martha and Ayers, Michael, *Cyberactvism: Online Activism in Theory and Practice*, New York and London: Routledge, 2003.

Qiu, J.L. *Working-Class Network Society: Communication Technology and the Information have-less in Urban China*, Cambridge, Massachusetts and London: The MIT Press, 2009.

Rozoff, Rick. “U.S. Cyber Command: Waging War in World’s Fifth Battlespace”, May 26, 2010, http://rickrozoff.wordpress.com/2010/05/26/u-s-cyber-command-waging-war-in-worlds-fifth-battlespace/

Smith, Michael and Warren, Peter. “NATO warns of strike against cyberattackers”, *The Sunday Times*, 6 June 2010, http://www.timesonline.co.uk/tol/news/world/article7144856.ece

Stahl, Roger. *Militainment Inc.: War, Media and Popular Culture*, London and New York: Routledge. 2010.

Wall, David, *Cybercrime: The transformation of crime in the information age*, Cambridge: Polity, 2007.

Van de Donk, Wim, Loader, Brian D., Nixon, Paul, G and Rucht, Dieter. (eds). *Cyberprotest: New Media, Citizens and Social Movements*, London and New York: Routledge, 2004.

Ventre, Daniel, *Information Warfare*, Wiley-ISTE, 2009.

Yang, Guobin, *The Power of the Internet in China: Citizen Activism Online*, New York: Columbia University Press, 2009.

[1] Athina Karatzogianni, “Confronting internal and external problems of cross- inter- and multi-disciplinarity: Researching cyber conflict and global politics” in Maria Karanika and Rolf Wiesemans (eds) *Exploring Avenues to Cross-Disciplinary Research*, Nottingham University Press, 2009b.

[2] For an example of the diversity of contributors and areas of study see Athina Karatzogianni (ed.) *Cyber Conflict and Global Politics*, (London: New York Routledge. 2009a).

[3] Athina Karatzogianni, *The Politics of Cyberconflict*, London and New York: Routldge, 20

[4] John Arquilla, and David Ronfeldt (eds.) *Networks and Netwars: The Future of Terror, Crime and Militancy*, (California: Rand, 2001).

[5] See Karatzogianni 2009a.

[6] Lincoln Dahlberg and Eugenia Siapera (eds.), *Radical Democracy and the Internet*, (Basingstoke: Palgrave Macmillan, 2007). For conflicts relating to peer production and the open source, see Athina Karatzogianni, and George Michaelides, “Cyberconflict at the Edge of Chaos: Cryptohierarchies and self-organization in the open source” in Phoebe Moore and Athina Karatzogianni (eds.) *Parallel Visions of P2P production: Governance, Organization and the New Economies,* Special issue*, Capital and Class*, 143-159 January 2009.

[7] Central European University. Participants’ reflections on workshop themes. “Cybersecurity: Europe and the Global Society Revisited: Developing a network of scholars and agenda for social science research on cybersecurity”, 7-8 June 2010, Budapest Hungary, http://ww.cmcs.ceu.hu/cybersecurity/main. Also see Andrew Liaropoulos, “War and Ethics in Cyberspace: Cyber-Conflict and Just War Theory”, Proceedings of the 9th European Conference on Information Warfare and Security, University of Macedonia, Thessaloniki, Greece, 1-2 July 2010.

[8] Smith, Michael and Warren, Peter. “NATO warns of strike against cyberattackers”, *The Sunday Times*, 6 June 2010, http://www.timesonline.co.uk/tol/news/world/article7144856.ece

[9] Athina Karatzogianni and Andrew Robinson, *Power, Resistance and Conflict in the Contemporary World*, (Routledge: London: New York, 2010), 115.

[10] Guobin Yang, *The Power of the Internet in China: Citizen Activism Online*, (New York: Columbia University Press, 2009).

[11] J.L. Qiu, *Working-Class Network Society: Communication Technology and the Information have-less in Urban China*, Cambridge, (Massachusetts and London: The MIT Press 2009).

[12] For an enjoyable tour of K5, see Bobbie Johnson, “No one is ready for this”, *The Guardian*, April 16, 2009, http://www.guardian.co.uk/technology/2009/apr/16/internet-hacking-cyber-war-nato

[13] Rick Rozoff, “U.S. Cyber Command: Waging War in World’s Fifth Battlespace”, May 26, 2010, http://rickrozoff.wordpress.com/2010/05/26/u-s-cyber-command-waging-war-in-worlds-fifth-battlespace/

[14] ibid.

[15] Heidi and Alvin Toffler, *The Third Wave*, Bantham Books, 1980.

[16] Arquilla and Ronfeldt 2001.

[17] Phillip Hammond, *Media, War and Postmodernity*, (London and New York: Routledge. 2009).

[18] Roger Stahl, *Militainment Inc.: War, Media and Popular Culture*, (London and New York: Routledge. 2010).

[19] James Der Derian. *Virtuous War* (London and New York: Routledge. 2009).

[20] Stahl.

[21] Hammond.

[22] Stahl.

[23] Der Derian.