SOCIAL REORDERING IN CYBER ERA

Tsirigotis Anthimos Alexander
(Researcher, M.Sc International and European Studies in the University of Piraeus, Greece)

At the dawn of the 21st century, "cyber" seems to have become the common prefix of every human activity expressing the tendency of people towards networking. Cyber world has emerged in parallel with the real world and its dynamic is so intense that many pundits consider it to be the fifth dimension in addition to land, sea, air and space. States throughout the world have expressed their vested interest in "armoring" their cyber dimension against intruders who intend to harm their vital interests. Networks of any nature (as for instance financial, political and social) have emerged as tools in the hands of anyone willing to take part in them regardless of their country of origin, mother tongue, religious belief or race. They seem to be supranational and many analysts describe networks as virtual societies that exist even though they cannot be defined using real life terms such as land or frontiers. It is interesting to think that many people spend a big part of their day "surfing" the virtual world rather than the real one. They are interlocutors in a worldwide chatting room of a society without borders, without limitations and with free flow of information; citizens of a virtual society with no or limited physical touch. This paper focuses on another aspect of cyber, laying emphasis on its societal dimension and potential to lead to worldwide reordering of power. It is suggested that cyber stems directly from societies and that it involves a different way of international societal organization. Cyber is not considered to be just a technological breakthrough. Instead, it is viewed as the next step to international organization. As chaotic and anarchical as it may be, cyber space is alleged to be the next form of international order.

Keywords: Cyber, cyber conflict, cyber war, Virtual Society

1. The cyber dimension of modern societies

Cyber seems to have become a common prefix that even though a considerable percentage of people has heard about, they cannot even give a rough definition of what it encompasses. This statement is not the official result of a scientific investigation but just a sensation judging mostly, on the one hand, by the increasing number of people who depend on Internet and, on the other, by the incidents of malicious behaviour to the detriment of domestic users. The recent report of Norton Group[1] leaves no room for doubt: *"65% of adults worldwide have been a victim of cybercrime"* (Norton, 2010: 4), by cybercrime meaning, for the purposes of the study, computer viruses/malware; online credit card fraud; online hacking;

[1] The research was conducted by Norton Group among more than 7066 adults from fourteen countries. The results were published in February of 2010 and its aim is to "*expose the alarming extent of cybercrime and the feelings of powerlessness and lack of justice felt by its victims worldwide. It identifies people's intense emotions towards the perpetrators and the often flawed actions people take to prevent and resolve cybercrime. The study nails down the true cost of cybercrime while raising questions about people's own online ethics and behavior."* (Norton, 2010:3). *Contact Mr. A. Tsirigotis at:* anthimostsiri@yahoo.gr

online harassment; online identity theft; online scams (as for instance fraudulent lotteries/employment opportunities); online sexual predation and phishing[2].

Incidents with wider repercussions that affect the whole societal body of targeted states are those of Estonia and Georgia as early as in 2007 and 2008 respectively[3]. These two cases are classified as the first cases of cyber attacks that concentrated the world's attention for revealing in the most blatant way the potentials of cyber dimension for military purposes. It is worth pinpointing that cyber attacks against governmental and financial Estonian networks were not combined with kinetic military attacks whilst in Georgia this was not the case. In Georgia cyber attacks were incorporated in military action plans and were executed in coordination with them. The Estonia and Georgia cases express two different perceptions of how the so called "cyber attacks" can be waged: as part of kinetic military operations or separately and exclusively with no need for any other military action.

More recently, in 2010, the WikiLeaks case but also the attack against an Iranian nuclear plant using the Stuxnet worm (McLynne, J.A., 2010) are distinguished among a series of daily (emphasis added) cyber incidents because they reveal what lies ahead. WikiLeaks may be the proof of *"how easily words that have legal meanings can be indiscriminately applied to cyber events in ways that can confuse decision makers and strategists alike"* (SSI Quarterly, 2011: 81). Additionally, the Stuxnet worm is the concrete example of how an industrial network of critical importance, which is considered to be closed (with no communication with the Internet) and thus secured can be compromised and finally forced to stop working (SSI Quarterly, 2011: 33-58). After the Stuxnet incident many countries have to be sceptical about the degree of concealment of their critical infrastructure and their ability to intercept any cyber attack coming out of the blue by invisible foes.

Cyber incidents really abound[4]. The above mentioned give the general view of what is happening and they are different aspects of the same reality which is currently brewing. All these cases may differ to the ways and to the degree they interfere with societal security and prosperity but in each one of them perpetrators launched "attacks" against targeted groups (individuals or even whole nations) not through air, land, sea or even space. Instead, they attacked through the cyber medium. Here lies the new reality whose dynamic is so potent that it leads to sea changes not only in the way people interact but also in the way societies communicate with each other. Inevitably, war as a communicational means among societies, albeit an extreme one, cannot be excluded from this process of change. Before giving my view about what cyber war is, it is useful to shed some light on what cyber really is. Is it a new dimension of the physical world in addition to land, sea, air and space? How does the cyber world force us to rethink of the real world or how does it induce us to redefine the physical world? The well defined principles of the real world as for instance sovereignty, nationality, borders and law how much applicable are they to the cyber way of life?

[2] For a comprehensive study of on line attack methods you can see: Won Kim, Ok-Ran Jeong, Chulyun Kim, Jungmin So (2011), "The dark side of the Internet: Attacks, costs and responses", *Information Systems vol.* 36, pp. 675–705.

[3] In Estonia cyber attacks were first launched at 27 of April until the 18th of May of 2007 as a protest to the decision of government to relocate a Soviet-era WWII memorial from a central location in the capital city to a military cemetery. In Georgia cyber attacks took place from the 8th until the 28th of August of 2008 and they were part of the military operations between Georgia and Russia. For further analysis see Tikk, E., Kaska, K., and Vihul, L. (2010) *International Cyber Incidents, Legal Considerations*, CCDCOE, Tallinn.

[4] Eric Sterner gives a concise review of cyber incidents in critical infrastructure and in military sector as well (SSI Quarterly, 2011: 62-64).

2. **Is there life in (cyber) space?**

For more than half a century now, the question whether there is life in space or not has attracted scientific interest. In just the first decade of the new century, social reality gives answer to a new and quite puzzling question whether there is life or not within cyber space. Cyber space was first born in human imagination in the 80's[5]. Since then, the rapid technological breakthroughs in informatics and especially the advent of the World Wide Web made it possible for cyber space to emerge. Societies do not thrive any more only in the three dimensional world but in a new dimension as well: the Infosphere. This one composed by various computer networks where people from any part of the world are present regardless of their social power or of any discriminating factor whatsoever. A new kind of society does emerge which seems to be seamless and to which the "product" of interest is nothing more than information, just like agricultural or industrial products used to be some decades before (Slaughter 2004).

It seems that a new social body is growing flesh and bones in parallel with or in some cases above sovereign states and their "official" societies. This is what I consider to be virtual societies which cannot be dimensionally defined and their members may never meet each other in real life. Nevertheless, they exchange their ideas, their worries and many of them (especially the younger ones) develop their basic human emotions, even love, for other human beings through the Internet! Cyber space constitutes a non material area of action, which should not be mistakenly interpreted as part of real life. Yet, it should not be conceived as a product of real life world that exists by virtue of it. Carr underlines that: *"The temptation to classify it as just another domain, like air, land, sea, and space, is frequently the first mistake that's made by our military and political leaders and policy makers. I think that a more accurate analogy can be found in the realm of science fiction's parallel universes—–mysterious, invisible realms existing in parallel to the physical world, but able to influence it in countless ways"* (2009: xiii).

Cyber world[6] is thriving as an autonomous space which is governed by its own principles that have nothing to do with the real world's ethical system of values. In the core of this new world is the flawless operation of networks of any kind and the uninterrupted information flow in the absence of any discriminatory factor (Slaughter, 2004; Castells, 2001; Arquilla, Ronfeldt, 1997)[7]. Anarchy is its fundamental organizational scheme (Arquilla, Ronfeld, 2001) while the real world follows hierarchies. Definitely, there is life in cyber space and this becomes more and more obvious as time elapses. Social networks (Twitter, Facebook et.al.) leave no doubt about that. People seem to be continuously connected to an invisible societal body wherever they may be on earth[8].

[5] The notion of cyberspace was first introduced in the cyberpunk science fiction book of William Gibson "Neuromancer" (Gibson, 1984). Trying to describe cyberspace Gibson defines cyberspace as *"A consensual hallucination experienced daily by billions of legitimate operators, in every nation, by children being taught mathematical concepts. ... A graphic representation of data abstracted from banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding."* (Gibson, W. 1984: 69).

[6] For the purposes of this paper cyber space and cyber world are considered to be the same.

[7] Arquilla and Ronfeldt pinpoint that *"Information is becoming a strategic resource that may prove as valuable and influential in the post-industrial era as capital and labor have been in the industrial age"* (1997: 25).

[8] The following extract is taken from a group of Facebook and it expresses in the most crystal clear way the core ideology of virtual societies: *"Sit comfortably in your desk chair, your sofa, your bed or even your local café and follow our game while you are updating your TWITTER, chatting on your SKYPE, spying your friends on FACEBOOK, or just searching something on GOOGLE…".*

What if the physical world decided to unplug all its networks? How dependent is cyber reality on the physical world? There are voices supporting that cyber world is overestimated (Dworschak, 2010; Harper, 2009; Isenberg, 2009). To deny the dependence of many human activities on networks as for instance of the financial system would be unrealistic. Still, over and above this, to say to young people that they have to abandon their smart phones or their i-Pads and stop having access to the Internet, that scenario, in my view, is inconceivable to them. As exaggerated as it may sound, for young people life cannot be conceived without being able to have access to the Internet. And that is not just a trend. Instead, it is their attitude towards life[9].

3. Cyber as proposal for international power reordering

Throughout history societies have been fighting each other in order to assert their political and physical independence in world politics. In 1648, the Westphalia treaty laid the legal foundations on which the international system since then has been working. The sovereign state was recognized as the principal political entity in international politics and national frontiers were established once and for ever. Change in real life has always been a strenuous, time consuming and really bloody process.

Nevertheless, in cyber world change seems to be rapid and bloodless. But how really an *"operational domain framed by use of electronics to …exploit information via interconnected systems and their associated infra structure."* as defined by Daniel T. Kuehl (in Kramer, F., Starr, S., Wentz, L., 2009:28) can change the real world? To conceive the cyber world exclusively through the lens of technology can be misleading. Cyber is not just a pioneering medium of communication. Cyber (without using the word as prefix to anything) constitutes the new proposal for international reordering which stems not from sovereign governments (from above), not even from each single society. Instead, and here lies the power of cyber, it stems from various people who live in different places within the three dimensional world, belong to different societies, have different mother tongues, do not share same religious beliefs, have different ages and they have never met each other! These are the citizens of virtual societies who thrive within cyber world and not in the material one[10].

Cyber expresses the new communicational environment that connects people. It is the leading power of change because it is open to anyone willing to take part in it. It is interesting to note that many times people in real societies feel that they are not able to express themselves or make a difference. Virtual societies do give them this opportunity. Their anger or their opposition to what is happening in real world politics, as for instance, to injustice, to frustration of any kind and to corruption are expressed through cyber. This is how cyber interferes with real life politics and finally provokes changes. The case of social upheaval in the Arab World is the concrete proof of the dynamics of cyber world to instigate change in real life politics (Lynch, M., Glasser, S.B., Hounshell, B. ed, 2011).

It would not be wise to state that cyber as organisational scheme of world politics will substitute sovereign state. On the other hand, anyone who tries to deal with cyberspace using the terms of the Westphalia era is not able to grasp the wind of change. As Nye notes: "*Cyberspace will not replace geographical space and will not abolish state sovereignty, but the diffusion of power in cyberspace will coexist and greatly complicate what it means to exercise power along each of these dimensions".* (Nye, JR., J., S. 2010: 3).

[9] For some people virtual life within cyber world is their unique option. The book of Tapscott (1998) is really interesting as it gives some facts and personal testimony of people who are living in the three dimensional world and in the cyber one in parallel.

[10] The advent of broadband service delivered via undersea cables will offer to much more people access to global networks enhancing the potentials of virtual society (J.Carr, 2009).

4. War in Cyber Era

War, as much criticism as it may receive, always constitutes an option for sovereign states, even one of last resort, in order to subjugate their adversaries. War, as defined by Clausewitz, constitutes one of the tools at the disposition of political powers in order to achieve specific political ends that society defines. Warfare, in its essence, has always been a means of communication among political entities which is shaped by the interaction of different forces inside of each one of the belligerent societies. The view of the war solely through the lens of a techno militaristic approach is at least misleading and dangerous to be used by strategic analysts. War remains an activity brewed within societies under the influence of the entire spectrum of societal powers. Brian M. Downing reiterates fervently that […] "*military organisation has been one of the basic building blocks of all civilizations, quite as important to political development as economic structures"* (Downing 1992).

What about war in cyber era? Are virtual societies inherently pacific? Definitely not. War as political praxis and as a means of communication is always an option of virtual societies as well. Virtual societies do fight each other but they also attack against sovereign states. Following the trend of the last decade, the prefix "cyber" has been added also to "war". "Cyber war", as a term, has ended up enclosing any kind of attack against networks (civilian and military as well) that aims at meeting any purpose (economic fraud, national security, espionage) and for which may be responsible a group of some youngsters with no malicious intents or a group of patriotic hackers or the so called cyber militias gaining or not official support (Carr, J. 2009). It seems that in cyber era bellicosity is inherent to the chaotic nature of networks. Networks of any nature are under attack every single day and systems designated to defend them are vigilant all the time. In virtual societies there is no official declaration of war as in real life.

The discourse about cyber warfare is actually vivid and interlocutors exchange diverse points of view as far as the legal context is concerned. Issues like what constitutes an attack in cyber space, what are its ethics and its law frame and furthermore its potentials as a means of meeting specific political ends are only some of the topics open to discussion (Janczewski, Colarik 2008). Even the definition of cyber warfare is not a topic of consensus and different opinions may be found reading the voluminous literature. Among them, the definition of cyber warfare by Jeffrey Carr as […] *"the art and science of fighting without fighting; of defeating an opponent without spilling their blood"* as much vague as it may seem it encloses the core of the issue. Martin Libicki, as early as in 2000, considers […] "*information terrorism, semantic attacks, simula-warfare, and Gibson-warfare"* constitute some of the aspects of cyber warfare underlying that it certainly is […] "*the least tractable because by far is the most fictitious, differing only in degree from information warfare as a whole."* (Gongora, Riekhoff 2000).

5. War in Cyber era: Some misunderstandings

To use the prefix "cyber" in order to describe what shape war takes may be misleading. War as a violent act among humans (following the theory of Clausewitz) is subjected to the powers of change of each era. Military technology has always been boosting new war paradigms as for instance railway, telegraph, RADAR and jet aircraft have changed once and for ever the conduct of war. In contrast, cyber is not a term used just to describe a breakthrough of Information Technology (IT). Cyber, as expressed earlier, is a new way that societies have spontaneously found in order to organize themselves above and beyond their official governments. Thus, to use the term cyber war in reference to a new war paradigm of the 21st century seems not to be appropriate.

Without doubt, military networks are not exempted from the target list of cyber attackers. In 1994, according to USA DoD, attacks against military networks were only 225. In just five years they reached 22.000 (Adkins, 2000: 1)[11]. Recently, PandaLabs announced that every week 57000 directions in Internet are hacker victims (in Writers, 2010). Moreover, the article of the New York Times: “Twitter Attack by Iranian Cyber Army” (Mackey 2009) demonstrates that in cyber space “armies” constitute already a reality and that they assume responsibilities on behalf of their states-bodies. It seems that in the 21st century, contrary to what happened in Early Modern Europe, the state gradually loses its power as the only legitimate body within societies able to secure its citizens (Münkler 2002).

Nevertheless, attacks against military networks cannot be classified as cyber war. Whenever a military network is compromised this is not an act of cyber war. Instead, it is Computer Network Operation (CNO) which gain support because of the extensive dependence of military operations on network-centric operations. Moreover, whenever bank networks are hacked this is not cyber war. It is just a new way of financial fraud to the detriment of consumers. Additionally, the defacement of governmental web pages or the disclosure of confidential documents (WikiLeaks case) cannot be considered to be acts of cyber war.

Virtual societies in cyber era are extremely prone to use cyber space without respecting any legal obligation in the real world. The limited regulated cyber space (or not regulated at all) gives chances to anyone willing to harm individuals, military organizations or sovereign states but this is far from constituting an act of war. Cyber space is inherently conflicting and anarchical. Thus, it seems more appropriate to use the term “cyberred conflict”[12] instead of cyber war for every day incidents that come to light and concern the misuse of cyber space. In cyber reality virtual societies are constantly in conflict and it is difficult to distinguish between conflict and war. Sovereignty, frontiers, boundaries, legislation and regulation are some of the principles of Westphalian societies that are refuted into cyber societies and which have to be redefined.

6. Some closing notes: The way ahead

To conclude, cyber is not to be used as just a prefix indicating the use of internet for the accomplishment of economic transactions, the exchange of some e-mails or the disclosure of confidential information. Cyber is the way people of different societies find to express themselves in favour of or against what is taking place in the real world. Cyber space enables any societal force of the real world to emerge, to inspire more people and finally to demand changes. Cyber is a proposal for international power reordering. Sovereign states have two options: either to suppress the dynamic nature of cyber space or to try to grasp the wind of change and to revise the international system as it has operated since the Westphalia era.

Progressively, the first option seems to gain vigour and many analysts advocate more strict regulation of Internet (SSI Quarterly: 32-61). Whilst the effort of every state to secure

[11] In 2007, the DoD of USA identified 43,880 malicious attacks against itself, rising to 54,640 in 2008 and 43,785 just through the first half of 2009. The defence secretary’s unclassified e-mail account was breached, and department officials report hundreds of thousands of cyber probes each day. Additionally, in 2007, NASA and the Departments of State, Homeland Security and Commerce all reported major intrusions resulting in lost data and interrupted operations (in SSI Quarterly, 2011:64)

[12] The term “cyberred conflict” is introduced by Demchak, C. and Dombrowski, P. as: *“Any conflict of national significance in which key events determining the path to the generally accepted outcome of the conflict could not have proceeded unless cyber means were nonsubstitutable and critically involved”* (SSI Quarterly, 2011: 58).

its prosperity in cyber era must be a concern of theirs, any effort to control the Internet is not a viable solution. The solution to the problem of state vulnerability to cyber attacks is not to "import" the principles of Westphalia era to the cyber one. The discourse about imposing virtual borders on internet or the continuous control of internet flaws (as those in China[13]) is anachronistic. The anarchy of cyber space is its power and states too have to take advantage of it rather than try to eliminate its dynamic.

[13] In China "*They built the "Golden Shield" that employs an estimated 40,000 Internet police who in 2009 shut down about 7,000 websites, deleted 1.25 million pieces of information, and arrested 3,500 people, including 70 dissidents and bloggers now in jail. In addition to directly controlling the content, about 30,000 netizens are employed part-time to intervene in online forum discussions and redirect conversations away from sensitive topics.*" (SSI Quarterly, 2011:45).

7. References:

Adkins, B.N. (2001) *The Spectrum of Cyber Conflict. From Hacking to Information Warfare: What is Law enforcement's Role?*, Alabama: Air Command and Staff College, Air University.

Arquilla, J., Ronfeldt, D. (1997) *In Athena's Camp: Preparing for Conflict in the Information Age*, National Defense Research Institute, Washington, D.C.: RAND.

Arquilla, J., Ronfeldt, D. (2001) *Networks and Netwars: The future of Terror, Crime and Militancy*, National Defense Research Institute, Washington, D.C.: RAND.

Boot, M. (2006) *War Made New. Technology, Warfare, and the Course of History. 1500 to Today,* Penguin Group, New York.

Carr, J. (2009) *Inside Cyber Warfare: Mapping the Cyber Underworld*, O'Reilly, USA.

Castells, M. (2001) *The Internet Galaxy. Reflections on the Internet, Business and Society*, Oxford University Press

Clausewitz, C. (1982) On War, Penguin Group, London.

Der Derian, J. (2009) *Virtuous War: Mapping the Military-Industrial, Media-Entertainment Network,* Routledge, New York.

Downing, B. M. (1992) *The Military Revolution and Political Change in Early Modern Europe,* Princeton University Press, Oxford.

Gat, A. (2001) *A History Of Military Thought: From The Enlightenment To The Gold War,* Oxford University Press, New York.

Gongora, T., Riekhoff, H. (ed) (2000) *Toward a Revolution in Military Affairs? Defence and Security at the down of the 21st century,* Greenwood Press, USA.

Janczewski, J., Colarik, A.M. (ed) (2008) *Cyber warfare and Cyber terrorism,* Information Science Reference, UK.

Kramer, F.D., Starr, S.H., Wentz, L.K. (ed.) (2009) *Cyberpower and National Security,* Centre for Technology and National Security Policy, Washington, D.C.: National Defense University.

Lynch, M., Glasser, S.B., Hounshell, B. (ed.) (2011) *Revolution in Arab World,* Foreign Policy, Washington Post Company.

Mackey, R. (2009) *"Twitter Attack by Iranian Cyber Army",* [on line], Available: http://thelede.blogs.nytimes.com/2009/12/18/twitter-hacked-by-iranian-cyberarmy/?scp=4&sq=Twitter%20Hack&st=cse.*2050* [20 Dec 2009].

McLynne, J.A. (2010) *"Stuxnet Computer Virus Made to Attack Iranian Nuclear Reactors?",* [on line], available: http://www.associatedcontent.com/article/5817134/stuxnet_computer_virus_made_to_attack.html?cat=15 [22-09- 2010].

Moskos, C., Williams, J.A., Segal, D. R. (2000) *The Postmodern Military: Armed Forces after the Cold War,* Oxford University Press, New York.

Münkler, H. (2002) *Die neuen Kriege*, Rowohlt Verlag GmbH, Reinbek bei Hamburg.

Nay JR., J., S. (2010) *Cyber Power,* Harvard Kennedy School, Cambridge.

Norton (2010) "Norton Cybercrime Report: The Human Impact", USA: [on line], available: http://www.symantec.com/content/en/us/enterprise/other_resources/b-symc_intelligence_quarterly_apr-jun_2010_21072009.en-us.pdf [10-09-10]

Rogers, C. J. (ed) (1995) *The Military Revolution Debate: Readings On The Military Transformation Of Early Modern Europe*, Westview Press, USA.

SSI Quarterly

Slaughter, A.M. (2004) *A New World Order,* Princeton University Press, USA.

Tapscott, D. (1998) *Growing Up Digital,* New York: McGraw-Hill.

Tikk, E., Kaska, K., Runnimeri, K., Kert, M., Taliharm, A., Vihul, L. (2008) “Cyber Attacks Against Georgia: Legal Lessons Identified”, Tallinn: CCDCOE, available: www.carlisle.army.mil/DIME/documents/Georgia%201%200.pdf [25-11-09].

Toffler A. (1991) *Powershift: Knowledge, Wealth and Violence at the Edge of the 21st century,* Bantam Books, USA.

Writers, S. (2010) “*Hackers make 57,000 booby-trapped websites weekly: Panda”,* Space Daily, [online], avalaible: http://www.spacedaily.com/reports/Hackers_make_57000_booby-trapped_websites_weekly_Panda_999.html [09-09-2010].