THE INVISIBLE CYBER WAR

Yiannos Charalambides[*]

Introduction

The international system is still dominated by sovereign nation states which constitute the main structural actors of the global system. However, nation states are not the only players acting in the global landscape. Markets or multinational colossi, even terrorist organisations such as Al Qaeda also operate in the international field (Charalambides, 2013, pp.71-77; Katzman, 2005 pp.4-5, 7-8; Bjelopera, 2011 pp. 36-37) with the purpose of changing the structure of the international system. In this respect, these international actors pursue to replace the dominant role that states retain in the international arena (Charalambides, 2013, pp. 71-75, 45-52). Technology constitutes one of the main constituent elements of power and therefore what remains to be examined is the role that technology can play in the international system in terms of the power game that is evolving. (Charalambides, 2010, pp. 34-35; Ifestos and Platias, 1992, pp. 83-84; Morgenthau, 1978pp. 9-14; Dougherty and Pfaltzgraff 1992, p 115).

This article deals with the importance of technology in the current era and particularly in the context of a new type of war, namely cyber war. This type of war is relevant to structural changes occurring in the

[*] Doctor of International Relations and European Studies.

international system, with technology playing its own significant role (Charalambides, 2013 pp. 12-13).

The present analysis refers to the various types of wars and attempts to give a definition regarding cyber warfare and explain how it works in practice. In this respect, we examine the way that cyber war affects the evolution of the international system and the resultant structural changes as well as the significance that cyber war plays in the international arena along with technology. In this reality, a relevant question which is raised and that we must answer is the following: whether the classical structural components of strength such as military power, territory and population size, the morale of the army and leadership are enough for a victorious outcome or whether technology itself and/or in combination with other means may bring dramatic changes regarding the component structure of wars and the structure of the international system (Charalambides, 2010 Dougherty and Pfaltzgraff 1992, p. 168; Gilpin 1981). So far, Great Powers seem to be invincible. However, two relevant questions must be answered: whether this hypothesis is correct and whether technology could increase the possibilities of restoring the old legend of David who defeated Goliath.

1. Various types of wars

In the current period, the international system suffers from various types of wars.

Firstly, classical wars in which the parties involved use conventional or even nuclear military means. It is a war that erupts between two or more states. Civil and/or religious wars –like the one ongoing in Syria (CNN News, 2012; CNN News, 2012a; CNN News, 2012b) - are included in the category of classical wars and usually induce such struc-

tural changes within the states that affect international affairs either in a regional or global level. Egypt constitutes an example through which we can observe the consequences of an uprising which brought about structural changes. Although Mubarak's regime had been constructed on a basis of deficient democracy, it succeeded to become a stabilising factor in the regional and global system. Mubarak's regime worked hard to achieve the consolidation of stability and peace with neighbouring Israel. When the regime fell, tensions erupted across the border with Israel (CNN, 2011, Charalambides 2012, p. 6). On June 24, 2012 the leader of the Muslim Brotherhood, Mohamed Morsi was officially declared as the winner of the first free Egyptian Presidential elections by a narrow margin over Ahmed Shafik. President Morsi gained 51,7% of the vote, while Ahmed Shafik received 48, 2% (CNN News, 2012c; BBC News, 2012). The political situation is volatile and both the US and Israel are concerned about the political, social and institutional role that the Muslim Brotherhood holds within the new Egyptian political system. The question is whether the uprising of the Egyptian people will lead to the establishment of a democratic political system or whether the Muslim Brotherhood will attempt to consolidate a political system, which would be based on and ruled by Islamic Law. Egypt is suffering political instability and runs the risk of a civil and religious war. Hence, the situation in Egypt induced structural changes within the state and affected the stability of the regional system.

Secondly, war on terrorism constitutes a *sui generis* type of war between states and terrorist organisations such as Al Qaeda, whose main aim is to alter the current structure of the international system (Bin Laden, 2005; Almasmari, Jamjoom and Abedine, 2012). Simultaneously, we are witnessing a perpetual conflict between two types of

Globalisation; Western and Islamist. Regarding the latter there is no doubt that it aims at establishing a Global Caliphate (Elsea, 2007, pp. 10-15; Lecker 2008, pp. 251-253). The mentioned ongoing conflict also takes the form of a religious war.

Thirdly, war among states and markets led to the current economic crisis. The markets attempt to play a dominant role in the international system and are not invisible. Therefore a relevant question should be asked: what is the market? A short definition answering this question could be set as follows: it is a legal and economic process through which the rules of supply and demand come together to define and determine the market prices. The market is not an abstract set of factors and actors functioning in the international system. On the contrary, it is a vibrant organisation acting in the international system and it is comprised of:

1. All types of companies, (small, medium, large) enterprises and any other entities engaged in any commercial, economic or financial activity as well as the individuals who lead and manage companies and industries; namely owners, shareholders, managers and directors.
2. Productive powers (forces), which is the combination of means of production and labour (tools, machinery, land and infrastructure), as well as the human labour power (Marx 1955).
3. Capital and money are instruments used by entrepreneurs in order to generate profit, wealth and growth. However, they are also used by employees (civilians) and labour forces in general, as income (i.e. salary, interest income, dividends etc), in order to cover their consuming needs.

4. The banking sector, national, private and international banking institutions and bankers that play a key role in local and global financial affairs.
5. The Stock Exchange and stockbrokers.
6. International organisations, banks and groups of powerful countries regulating political and economic affairs such as the G-20, the International Monetary Fund, the Global Bank For Reconstruction And Development, as well as the World Trade Organisation (WTO).
7. All persons who are directly or indirectly involved in the market, such as lawyers, bankers, accountants, politicians, workers (labour force) and consumers, trade and labour unions and their members, politicians and political parties, ministers and governments. Most often - political parties, politicians and governments - are financially sponsored by the business world or civilians -namely bankers, businessmen or ordinary voters.
8. Energy – Power providers and all the factors that the power supply chain consists of. Both states and/or individuals provide conventional or renewable sources of energy, engineers and equipment so that energy arrives at the end-user destination (industrial units, households) and thereby the brokers define the exchange price of energy goods.
9. Research centres, universities and other forms of innovation providers, who can create new commodities or new ways of developing and thus enhancing, the quality of the products.
10. Central Governments which are obliged to provide security and stability to all entities performing economic and other activities in the context of the state's apparatus.

11. International and local financial and commercial laws and other regulators through which we can measure and evaluate the level of compliance between rules, laws, directives and regulations on the one hand and the level of actual implementation on the other.
12. "Credit Rating Agencies" which are authorised to evaluate and thus upgrade or downgrade private banks and the banking sector in general. In fact, they hold a key regulatory role in the global financial and political system (Standard & Poor's, Moody's and Fitch Ratings). The "Credit Rating Agencies" are used by investors, issuers, investment banks, broker-dealers and governments for security reasons in terms of protecting their financial interests and thus reducing the risk of their investment. In this respect, the "Credit Rating Agencies" draw up reports in which the credit risk is analyzed with the aim of protecting the investors and increasing the efficiency of the market. Due to the current economic crisis both the US and the EU (including its Member States) put in question the credibility of the "Credit Rating Agencies". Markets constitute vibrant organisations where human beings play, operate, act and react and thereby psychology is always turned into a political and economic instrument which might be used by the "Credit Rating Agencies" to influence markets in favouring "suspicious interests". The time and the way a report is drawn up, often set forth the economic and political situation of a state, its banking sector, financial status and its sovereign debt, affect either negatively or positively the market and the economy of state in question, as well as the markets in general.
13. Currency value and exchange rates as decisive instruments of the market and for financial transactions.

2. Definition of Cyber war

Beyond the types of wars mentioned above, another type of war is also noteworthy. It is the cyber war, which is inherent to technological development and is always used in the context of a wide range of wars. The actors involved in such a war use high level technologies. Cyber war is part of the wider electronic war and its technological capabilities are exploited as indispensable instruments for the victorious outcome of a classical, conventional or any other kind of conflict. In attempting to define what "cyber warfare" is, the U.S. government security expert, Richard A. Clarke maintains*:*

"When the terms of 'Cyber war' are used in this book, they refer to actions by a nation-state to penetrate another nation's computers or networks for the purposes of causing damage or disruption" (Clarke 2010, p. 6).

In addition, the *Economist* wrote that cyberspace constitutes *"the fifth domain of warfare" (in addition to land, sea, air and space)* (Economist 2010) and William J. Lynn, U.S. Deputy Secretary of Defense, underlines that *"as a doctrinal matter, the Pentagon has formally recognized cyberspace as a new domain in warfare. . . [which] has become just as critical to military operations as land, sea, air, and space" (Lynn 2010, p.97-98).*

These are some short definitions of cyber war. However, one could assert that cyber war cannot be precisely defined. Pursuant to a study requested by the Subcommittee on Security and Defence and issued by the European Parliament:

"*There is no common definition of what might constitute 'cyber warfare'. The 2007 attacks on Estonia, the 2008 attacks on Georgia, the deployment of Stunxet, or the ongoing high level cyber-espionage were*

all called cyber war at some point. Even cyber attacks that most likely have nothing to do with conflicts between states, such as 'hacktivism', or cyber attacks in the wake of the 2010 WikiLeaks affair, or in support of the February – March 2011 Arab revolts have been called cyber war, implying in effect that the concept of warfare is not limited anymore to mere nation – states. In the absence of a common definition, most of the EU Member States and the Commission have studiously avoided using the term cyber warfare in official documents and often prefer neutral such as 'cyber espionage', 'cyber attack' or 'cyber defence'" (European Parliament, 2012, p. 9) .

2.1. Various levels of cyber war

According to the so–called AF-SAB model there are three levels of military cyber attacks:

The First Level of military cyber attacks is the "network wars" or *"'system administrator versus system administrator'. This includes mobile malicious logic, Trojan attacks, basic phishing attempts, common exploits, website defacement and other common headaches falling within this category".* This category of attacks is the least serious, including *"purported state-sponsored espionage attacks on the government such as the 'Moonlight Maze' and 'Titan Rain' campaign". These attacks can be addressed by proper network security precautions"* (European Parliament, 2012, p. 7). "Titan Rain" was a sophisticated and cyber espionage attack which *"began in 2003 against the US and led to the wide-scale breach of classified US government and military systems, with loss of 10-12 terabytes of information" (European Parliament, 2012, p.52).* This attack and others had been organised and performed by non-state Chinese hackers. Over a four year period, they

launched similar attacks on government systems and EU member states and EU institutions. Albeit the attackers were not directly associated with the Chinese State, they probably cooperated with the Chinese Security Service as they were under an official command also having connections with high level political leadership.

The Second Level cyber attacks fall under "cyber - adjunct to kinetic combat". The operator attempts to achieve a "kinetic effect" in conjunction to a conventional attack, such as an air strike. Therefore, the operator uses malicious logic to defuse an air defence network. This example exemplifies level 2 cyber attacks (European Parliament, 2012, pp. 7-8). The 2008 cyber attacks on Georgia also fall under this category. These attacks had been combined with military conventional operations and therefore had a kinetic effect. During the war on Georgia, the Russians defaced websites whilst they also launched attacks on critical energy infrastructures. Another relevant case of Level 2 cyber war practice was the one between Syria and Israel in 2007, when the Israelis used the American cyber-weapon, named "Senior Suter", in order to defuse the Syrian Antiaircraft Network and successfully launched their airstrikes against Syria and precisely hit supposed nuclear facilities on the ground.

The last and Third Level is "malicious manipulation", which specialists consider as the most dangerous attacks. These attacks: *"are the ones to be feared, they are covert, they are planned, they are orchestrated and they can use widespread havoc and disruption without the victims realizing their problems are cyber related".*

According to a study issued by the services of the European Parliament, *"Level 3 attacks also conceal a wide range of possible behaviour – this can include the simple manipulation of a spreadsheet, to Stuxnet*

and similar purported limited attacks on critical infrastructure, to mass –casualty attacks on an entire nation's critical infrastructure or even the misrouting of the internet itself" (European Parliament 2012, p. 8).

It is of utmost importance to underline that with a reference to "Stuxnet" we mean a "cyber missile" which had been *"directed squarely at the Iranian nuclear program by targeting its uranium enrichment capability"* (European Parliament p. 52, The Economist, 2010). As the report of the European Parliament maintains: *"There has been clear evidence that Stuxnet was successful in damaging and delaying the Iranian enrichment program"* (European Parliament, 2012, p. 52, Farwell and Rohozinski 2011, pp. 23-40). This attack was not the first one which used the invisible "weapon" of high technology. As Thomas Reed underlines, an advisor to President Ronald Reagan alleged that the CIA used a logistic bomb in 1982 to destroy a Soviet pipeline and he adds:

"It was programmed to go haywire, to reset pump speeds and valve settings to produce pressures far beyond those acceptable to the pipeline joints and welds. The result was the most monumental non-nuclear explosion and fire ever seen from space" (Reed, 2004, p. 269).

2.2. American superiority

It is evident why the US is considered the champion state in cyber -warfare and cyber-defence. Beyond the cases mentioned above, in 1991, during the First Iraqi War, the US impressed the international community with its advanced skills of cyber-war. Years later, in 2010, NATO – led by US - was the first organisation that realised the necessity to address the "new threats" stemming from cyber-attacks. This necessity became more obvious after the 2007 attack on Estonia, which entailed web – vandalism. In particular, over a three week period the at-

tackers caused disruption to Estonian public services and banking sector. The attackers were probably Russian hackers and the attack was a strong shock for the international community. It was an episode that alarmed relevant stakeholders and led NATO to rethink and take pertinent decisions regarding its defensive strategic concept. At the Lisbon Summit in November 2010, NATO established the Cyber Defence Management Authority (CDMA), with the competence to coordinate and shape strategic decision-making on cyber-defence within the Alliance (European Parliament, 2012, p. 26, NATO 2010a). However, China and Russia are also involved in all levels of cyber-war, as they have no other alternative than to respond to the requirements of the contemporary era, in order to serve and protect their national interests by undertaking all kinds of preventive measures. In fact they not only defend themselves, but also follow an aggressive policy. In this respect, one should view cyber-attacks through the lens of political practices. Hereupon, we may underline that quantitative analysis of cyber-war cannot be focused exclusively on the three aforementioned levels, but also on the civilian, commercial, economic, administrative, banking or military sectors which the cyber-attacks usually target. In this respect, such a cyber trade-economic war is currently underway between China and the US. Pursuant to a congressional report titled "China-US Trade Issues", Wayne M. Morrison maintains:

"*Many U.S. analysts and policymakers contend that the Chinese government is a major source of cyber-economic espionage against U.S. firms. For example, Representative Mike Rogers, chairman of the House Permanent Select Committee on Intelligence, stated at an October 4, 2011, hearing that attributing this espionage isn't easy, but talk to any private sector cyber analyst, and they will tell you there is little doubt that this is a massive campaign being*

conducted by the Chinese government. I don't believe that there is a precedent in history for such a massive and sustained intelligence effort by a government to blatantly steal commercial data and intellectual property. China's economic espionage has reached an intolerable level and I believe that the United States and our allies in Europe and Asia have an obligation to confront Beijing and demand that they put a stop to this piracy".

According to a report by the U.S. Office of the Director of National Intelligence (DNI): "*Chinese actors are the world's most active and persistent perpetrators of economic espionage. U.S. private sector firms and cyber security specialists have reported an onslaught of computer network intrusions that have originated in China, but the IC (Intelligence Community) cannot confirm who was responsible." The report goes on to warn that "China will continue to be driven by its longstanding policy of 'catching up fast and surpassing' Western powers. The growing interrelationships between Chinese and U.S companies — such as the employment of Chinese-national technical experts at U.S. facilities and outsourcing U.S. production and R&D to facilities in China — will offer Chinese government agencies and businesses increasing opportunities to collect sensitive US economic information" (Morrison 2012, p. 33).*

2.3. China, Russia and hackers' army

China and Russia hold a privileged position in the list of the main global cyber powers, with a huge army of hackers operating particularly against US interests. Most of the hackers have no official relations with the Chinese or Russian governments. However it is a commonly known "secret" that the Chinese government has tacitly approved the hackers' attacks. The Chinese concept on Cyber-warfare, titled "Integrated Network Electronic Warfare", is similar to the US Network Electronic Warfare. In this context civilian sources (People's of war) are mobilised in order to attempt operating at a strategic level of conflict, namely

"information warfare". This information warfare is divided in three categories: Media warfare, Psychological warfare and Legal warfare (European Parliament, p. 55). The Chinese have a very strong system of defensive and offensive capabilities, whilst there is a real army, the "Patriot Hackers" which are responsible for the attacks against western governments and interests. The "Red Hacker Alliance" is the largest club of attackers, numbering 400,000 members. The Pentagon had to take special measures in order to prevent their attacks (European Parliament, 2012, p. 57).

Along the same lines, Russia is concentrated on the means and measures that it should take in order to protect its civil society, military/ governmental infrastructures and apparatus from US hackers. In terms of "soft and smart power" the US pursues to influence the Russian public opinion and furthermore the decision making process (Nye, 1991; Nye 2004, pp. 2, 34-35, 44-45; 2006; Crocker et al, 2007, p.13; Etheridge, 2009). This is a strategy named "reflexive control". In accordance with this concept *"one enemy transmits the reasons and bases for making decisions to the other" (Thomas 2004).* This is a strategic method through which the US influences certain public opinions that are under the pressure of authoritarian regimes, and pushes them to revolt. Iran and the Arab Spring constitute evident cases of this strategic method used by the US cyber-war services. All relevant information, reasons and data which can influence the procedure of the decisions taken by repressed public opinions are promoted through the cyberspace. Certainly, the result of this method, inherent to a "smart power" strategic concept, is not always positive. Beyond the influence that the US may exert over foreign public opinions, there are other factors acting in a society and within an authoritarian political system. These factors affect

the procedure of the decision making. Such a strategic goal becomes easier when the foreign public opinion is ready to adopt a propaganda promoted through the internet. The success or failure of this policy also depends on the skills of the intelligence services of the state being under the US attack. The key issue is whether they successfully react against such a "cyber war game". Therefore, the Russian information doctrine focuses on protecting the public opinion and the Russian "spiritual renewal" by establishing segments of "information psychological" and "information technical means" (Bikkenin, 2003).

3. A landmark case

The "WikiLeaks case", widely known as "Cablegate" – the publication of thousands of top secret US documents – shows the electronically sophisticated character of the new era; an era where technology constitutes a primary instrument for the secret services and for any other skilled person or organisation. The publication of numerous top secret documents (251,287 diplomatic cables) shed light on dimming aspects of secret diplomacy and illustrated how diplomats comment and evaluate each other behind the scenes (WikiLeaks 2012). On August 20, 2010, the Swedish prosecutor issued an arrest warrant against the founder of WikiLeaks, Julian Assange amid two accusations. One concerns the allegation of rape and the other of molestation. Assange denied the charges arguing that he was a victim of a smear campaign. The Swedish Authority requested his extradition from Britain where Assange found shelter in the embassy of Ecuador. Assange applied for asylum and the Ecuadorian Authorities on August 16, 2012 took a positive decision triggering a diplomatic episode with Britain. The Foreign Minister of Ecuador stated that his country granted asylum to Assange *"because he will be*

politically persecuted if extradited" (Lai, 2012). The British government was clear about its intention of arresting and extraditing him to Sweden. Assange feared he would be sent by the Swedish Authorities to the US where he might face the death penalty. The US Authorities accused him of publishing top secret cables (official US documents), putting the country's security at risk. On August 14, 2012, in an effort to explain the upcoming positive decision - which would be issued two days later - the Ecuadorian President Rafael Correa stated:

"The process in Sweden needs to be reviewed, you have to consider the possibility of extradition to the United States, if there's a secret tribunal there, if there's any risk of a death penalty. It requires a large amount of information, an analysis of international law to make an informed, absolutely responsible and sovereign decision" (Correa, 2012, cited in CNN Wire Staff 2012).

"WikiLeaks" cast a shadow on the US security system and humiliated the American secret services. It is in fact a landmark case which illustrates both the importance that technology plays in international affairs and the new types of wars which noiselessly occur not only among states, but also between states and non-state actors. In this case we observe the way technology pulverises the gap of strength existing between a Great Power and a private organisation of electronic media.

Conclusions

Technology constitutes a structural component factor of strength used by states in order to serve their national interests in the context of a trade/economic cyber war, like those underway between the US and China or the US and Russia, without excluding that other countries will also get involved. This is a conflict among the Titans of the interna-

tional system with the US playing the role of Zeus. Furthermore, technology and cyber war are also used in the frame of conventional wars and the war on terror. In fact, it is a combination of an economic/ commercial and cyber war upon which the new era is reflected. It illustrates how complicated international relations are in the contemporary period. It is evident that there are "two or three types of wars", one existing within the other, without the need to use the traditional, classical military means. Particularly, the Army uses cyber mechanisms as an indispensable tool for espionage purposes in the frame of a wider strategic plan with the aim of promoting and protecting national interests. In parallel, the tools and weapons of cyber war are also used in conventional wars. Advanced technology is always of outmost importance for the international actors in order to win a victory.

The international system is already in a new era in which structural changes occur and power coexists with technological development and capacities. An invisible cyber war, among Great Powers, such as the US, Russia and China is underway. Certainly, other countries, apart from Great Powers, are already involved in a cyber war for which new types of armies have been formed. Hackers now play the role of "modern soldiers", thus evincing the eminent importance that technology holds as an indispensable factor of national strength (Dougherty and Pfaltzgraff 1992, p. 116). In this reality, the structure and methods of wars tend to change along with the structure of the international system where the state still holds its dominant role. However, markets and terrorist organisations such as Al Qaeda spare no efforts to replace the states' dominant position. Through the lens of the "WikeLeaks case" we observe a new political phenomenon stemming from technology and reflecting the growing significance of technology and the changes oc-

curring in the international system where an electronic media non-governmental organisation got involved in a cyber war with the US. The US defeat until this moment is obvious. This incident brings to mind the well known story of David and Goliath. And thus history repeats itself by using other means. At that time, it was the sling and stones, nowadays it is technology.

May, 2013

References and Literature

1. *Almasmari, H, Jamjoom M and Abedine S* (2012) Yemen: Al Qaeda affiliate behind blast that killed 101 soldiers. CNN. May 22. Available from: http://articles.cnn.com/2012-05-22/middleeast/world_meast_yemen-violence_1_al-qaeda-al-sharia-president-saleh?_s=PM:MIDDLEEAST
2. BBC News (2012) *Muslim Brotherhood's Morsi declared Egypt president, June 24.* Available from: http://www.bbc.co.uk/news/world-18571580
3. *Bjelopera, P. J. (*2011) American Jihadist Terrorism: Combating a Complex Threat. Congressional Research Service. November 15. Available from: http://www.fas.org/sgp/crs/terror/R41416.pdf
4. *Bin Laden, O.* (2005) Interview Message to the World, Verso, October 21, 2001.
5. *Blanchard, C.* (2007) 'Al Qaeda: Statements and Evolving Ideology'. CRS Report for Congress. July 9. Available from: http://www.fas.org/sgp/crs/terror/RL32759.pdf
6. Centre for Defence Information. *Operation "Enduring Freedom"*. Washington. Available from: http://www.cdi.org/program/issue/index.cfm?ProgramID=39&issueid=48
7. CNN News (2012) Breaking News. *The speech that President Assad addresses the Syrian Parliament.* 3 June.
8. CNN News (2012a) *Kofi Annan resigns as envoy to Syria.* Available from: http://security.blogs.cnn.com/2012/08/02/kofi-annan-resigns-as-envoy-to-syria/
9. CNN News (2012b) A reportage on the TV (CNN International) which transmitted the message sent by the Syrian rebels of the "Syrian Liberate Army". The rebels called upon Turkey to military intervene
10. CNN News (2012c) *Muslim Brotherhood's Morsi declared Egypt's new president*. June 24. Available from: http://edition.cnn.com/2012/06/24/world/africa/egypt-politics/index.html?hpt=hp_t1

11. *Correa, R.* (2012) Cited in CNN wire staff. Ecuador: Decision on WikiLeaks founder's asylum request coming. August 14. Available form: http://www.cnn.com/2012/08/14/world/americas/ecuador-assange/index.html
12. *Charalambides, Y.* (2011) Cyprus Issue: Diplomatic Plots, top secret documents and testimonies from 1950 to 2010, Strategic deficits and options. Athens: Piotita.
13. *Charalambides, Y.* (2013) The Third World War, Global Titans and Sworn Soldiers. ERPIC, Nicosia.
14. *Clarke, R A.* (2010) Cyber War. The Next Threat to National Security and What to Do About. As imprint of HarperCollins Publishers.
15. *Crocker, A., Hampson, O. and Aall P.* (2007) Leashing the Dogs of War: Conflict Management in a Divided World. US Institute of Peace Press.
16. *Dougherty, J. and Pfaltzgraff R.* (1992) Contending Theories of International Relations: A Comprehensive Survey. Athens: Papazisis Publications, vol. 1.
17. Economist (2010) *"Cyberwar: War in the Fifth Domain".* 1 July. Available From: http://www.economist.com/node/16478792
18. European Parliament (2012) External Representation of the Euro Area. Directorate General for International Policies Policy A: Economic and Scientific Policy. A Study issued from the European Parliament. Authors: Alessandro Giovannini,
19. Daniel Gros, Paul Ivan, Piotr Maciej Kacznski, Iego Valiante. Available from: http://www.europarl.europa.eu/studies
20. *Elsea, Jeniffer K.* (2007) *Treatment* of "Battlefield Detainees" in the War on Terrorism. Updated January 23, 2007. CRA Report for Congress, order code RL 31367. Available from: http://www.fas.org/sgp/crs/terror/RL31367.pdf
21. *Etheridge, E.* (2009) How 'Soft Power' Got 'Smart'. The New York Times. January 14. Available from: http://opinionator.blogs.nytimes.com/2009/01/14/how-soft-power-got-smart/
22. *Farwell, J and Rohozinski R* (2011). 'Stunxnet and the Future of Cyber War'. Survival, Vol. 53(1), 2011.
23. *Gilpin, R.* (1981) War and Change in World Politics, Cambridge University Press, New York.
24. *Ifestos, P. and Platias A.,* (1992) Greek Preventive Strategy. Published by Papazisis, Athens.
25. *Karl, M.* (1955) The Poverty of Philosophy. Answer to the Philosophy of Poverty by M. Proudhon. Progress Publishers. First Publication in Paris and Brussels 1847. Available from: http://www.marxists.org/archive/marx/works/download/pdf/Poverty-Philosophy.pdf
26. *Katzman, K.* (2005) Al Qaeda: Profile and Threat Assessment. - CRS Report for Congress. Received through the CRS Web. August 17. Available from: (http://www.fas.org/sgp/crs/terror/RL33038.pdf)

27. *Lai, A.* (2012) Timeline: Julian Assange's extradition battle. CNN. August 16. Available from: http://www.cnn.com/2012/08/16/world/europe/assange-extradition-timeline/index.html?iid=article_sidebar
28. *Lecker, M.* (2008*)* "The 'Constitution of Medina': Muhammad's First Legal Document".Journal of Islamic Studies 19 (2): 251–253, DOI:10.1093/jis/etn021. Available from: http://jis.oxfordjournals.org/content/19/2/251
29. *Lynn, W. J. III* (2010) "Defending a New Domain: The Pentagon's Cyberstrategy". Foreign Affairs, Sept/Oct. 2010.
30. *Morgenthau, H.* (1978) Politics among Nations: The Struggle for Power and Peace. New York: Knopf.
31. *Morisson, M. W.* (2012) China-U.S. Trade Issues China-U.S. Trade Issues. Congressional Research Service. May 21. Available from: http://www.fas.org/sgp/crs/row/RL33536.pdf
32. NATO (2011) *Defending against cyber attacks*. NATO Homepage. Available from: http://www.nato.int/cps/en/natolive/topics_49193.htm
33. *Nye, J.* (1991) Bound to Lead: The Changing Nature of American Power. US: Basic Books
34. *Nye, J.* (2004) Soft Power: The Means to Success to World Politics, U.S: Public Affairs
35. *Nye, J. (*2006) In Mideast, the Goal is "Smart Power*". Boston Globe*. August 19. Available from: http://www.boston.com/news/globe/editorial_opinion/oped/articles/2006/08/19/in_mideast_the_goal_is_smart_power/
36. *Reed, T.* (2004) At the Abyss: An Insider's History of the Cold War. New York, Press.
37. *Tomas, T.* (2004) "Comparing US, Russia and Chinese Information Cooperation Concepts". Foreign Military Studies Office, February. Available from: http://www.dodccrp.org/events/2004_CCTS/CD/papers/064.pdf.
38. The Economist, (2010) *A cyber-missile aimed at Iran?* 24 September. Available from: http://www.economist.com/blogs/babbage/2010/09/stuxnet worm.
39. Wikileaks (2012) *Secret US Embassy Cables.* Available from: http://wikileaks.org/cablegate.html#