8 Explaining the use of the prefix Cyber-

Elizabeth Hatziolou, Stamatia Sofiou

ABSTRACT

The prefix *cyber-* is one of the most used prefixes in our information age. Scientists use it in their works; politicians employ it in official documents concerning problems to be solved, like economics, national security, terrorism and war; students are taught about it in technology classes, i.e. web blogs and websites; and the general public exploit it in order to benefit from it by exchanging information through speaking or writing. Such is the popularity of the prefix that it is being used by most people in the world most of the time. The reason is not difficult to comprehend. *Cyber-* is a prefix easy to remember and spell. Attached to the beginning of an old word it creates a new one with a different meaning, aiding people in communicating in different contexts. The result of the extensive use of the prefix was the coining of the term *cyberology*, meaning the study of the Net and its applications, like *cybernetics* and *cyborgs*, *cyberspace* and *cyber war* that enable the computer network to respond to threats to digital computers, either domestically or internationally. The study explains how the new *cyber-* vocabulary has developed through the decades (from the Sixties to the Two Thousands) and how the different types of *cyber-* words, i.e. *cyber cubicle*, *cyber repression*, *cyber deterrence*, *cyber toll*, *cyberocracy, Cyberia, cyberformance* or *cyber warfare*, to mention but a few, are being used in order to make our life and work easier.

KEYWORDS: Computer science, cyber culture, cybernetics, cyber security, cyborg, cyber risk, cyber war.

Εξηγώντας τη χρήση του προθέματος Cyber-

Ελισάβετ Χατζηόλου, Σταματία Σοφίου

ΠΕΡΙΛΗΨΗ

Το πρόθημα *κυβερνο-* είναι ένα από τα πιο συχνά χρησιμοποιούμενα προθήματα στον αιώνα της πληροφορίας που ζούμε. Οι επιστήμονες το χρησιμοποιούν στις ακαδημαϊκές εργασίες τους· οι πολιτικοί το μεταχειρίζονται στα επίσημα έγγραφά τους, που αφορούν στα προβλήματα που αντιμετωπίσουν, όπως είναι η εθνική ασφάλεια, η τρομοκρατία και ο πόλεμος· οι σπουδαστές διδάσκονται για αυτό στο μάθημα της πληροφορικής· και το κοινό το αξιοποιεί όταν ανταλλάσσει γραπτές και προφορικές πληροφορίες. Τέτοια είναι η απήχηση του προθήματος που ο περισσότερος κόσμος το χρησιμοποιεί κάθε μέρα. Ο λόγος είναι απλός. Το πρόθημα είναι εύκολο να απομνημονευτεί και να χρησιμοποιηθεί στον προφορικό και στον γραπτό λόγο επειδή όταν μπει στην αρχή μιας λέξης της καθομιλουμένης δημιουργεί μια καινούργια λέξη με διαφορετικό νόημα, βοηθώντας έτσι την επικοινωνία σε διάφορα επίπεδα. Το αποτέλεσμα της εκτεταμένης χρήσης του προθήματος ήταν η επινόηση του όρου *κυβερνολογία* που σημαίνει τη μελέτη του Δικτύου Η/Υ και των εφαρμογών του, όπως *κυβερνητική* και *κυβερνο-οργανισμός*, *κυβερνοχώρος* και *κυβερνο-πόλεμος*, που καθιστούν το δίκτυο ικανό να ανταποκρίνεται σε εγχώριες και διεθνείς απειλές στους Η/Υ. Η μελέτη εξηγεί πως το *κυβερνο-λεξιλόγιο* αναπτύχθηκε από τη δεκαετία του 1960 έως τη δεκαετία του 2000 και πως οι διαφορετικοί τύποι των καινούργιων όρων όπως, για παράδειγμα, *κυβερνο-δωμάτιο*, *κυβερνο-καταστολή*, *κυβερνο-αποτροπή*, *κυβερνο-χτύπημα*, *κυβερνο-κρατία*, *κυβερνο-τιμωρία*, *κυβερνο-απόδοση*

ή κυβερνο-πόλεμος χρησιμοποιούνται για να κάνουν την γραπτή και προφορική επικοινωνία ευκολότερη.
Λέξεις-Κλειδιά: Επιστήμη των Η/Υ, κυβερνο-κουλτούρα, κυβερνητική, κυβερνο-ασφάλεια, κυβερνο-οργανισμός, κυβερνο-διακύβευμα, κυβερνο-πόλεμος.

0 Introduction

The prefix *cyber-* is used in terms related to computers and the Internet. It comes from the Greek verb *κυβερνώ*, which means to 'pilot'. An example of how the prefix is used in Greek is the noun *κυβερνήτης*, meaning 'pilot'.

The prefix appeared in the early Fifties when a group of scientists in fields ranging from social sciences to engineering began to employ it in scientific works. Its extensive use resulted in the coining of *cyberology*, a term that means the study of the Internet and its applications. Since the Fifties the scientific field of *cyberology* has grown to include *cybernetics*, an interdisciplinary study concerning *control systems*, for example, a missile control system; *electrical network theory*, i.e. the collection of interconnected components; *mechanical engineering*, the discipline that applies engineering to design and manufacture; *evolutionary biology*, a subfield of biology that studies the evolutionary process producing the diversity of life on Earth; *neuroscience* or the scientific study of the nervous system; *anthropology*, the study of human behaviour and society in the past and present and *psychology*, concerning behaviour, conscious / unconscious phenomena and thought.

1 Main body

Cybernetics became important because the term reminded people that *cyber-* attached to the beginning of a word created a new word. So, the formation of new, compound words that included the prefix continued in the Seventies and Eighties to include a great deal of *temporary* or *nonce* words; *lexemes*, 'λεξήματα,' units of vocabulary that may exist in a number of different forms, e.g. 'play' existing as 'plays, playing, player, played'; and the different forms of *lemma,* 'λήμμα' or the headword of a dictionary entry, employed in order to solve problems of communication. For example, *cyber cubicle* was coined to mean a small area for private use in an Internet Café; *cybercafé* or *cyber pub* applies to Internet places and *cyber friend* means a friend with whom one communicates only through the Net; *cyber lover* implies a distance relationship and *cyber sex* is a situation in which two people

connected remotely through computer network send each other messages describing a sexual experience; *cyber party* refers to a political party whose relations to its supporters occurs through email or texting instead of being based on membership; *cyber snob* implies an individual who thinks that his / her knowledge of online items (jargon and acronyms) makes him / her an expert; and *cyber culture* is the culture arising from the use of computer networks for communication, entertainment and business.

In the urban subculture there developed terms, like *cyber goth* to refer to goth, rave and rivet head fashion, involving young men and women who listen to electronic music more often than rock music and buy attire from C*yberdog*, i.e. a shop in London that specializes in bright fluorescent clothing. In fact, the terms *cyber-sick* and *cyber tedium* appeared in the Eighties and Nineties to refer to the mass of derivative words that appeared after William Gibson (1948-) the Canadian-American writer invented *cyberspace* in his 1984 novel *Neuromancer* although he had already invented it two years previously in his short story called *Omni*. Even adverbs, like *cyberly* (as in "He's been harassing her cyberly") or *cyber-sheepishly*, meaning in a manner showing lack of self-assertion concerning the Net, and adjectives like *cyberish* (as in cyberish art or cyberish images) have been coined to help Internet users to exchange information.

Besides these compound words, there appeared others that relate to politics, espionage and war. *Cyborg*, combining the 'cyb-' of cyber with the 'org-' of organism, refers to a robot, a man-machine or android, capable of interacting in the environment for which it was built with the help of a neuron electrode that allows elaborate interactions. The term *cyborg* was first used in the Seventies in scientific publications and TV shows. In fact, instead of *cyborgs* the compound nouns *cyber men* and *cyber women* were used to refer to individuals with superhuman power (bionic implants) that were employed as spies by government agencies.

Another term that evolved through the use of *cyber-* and is associated with government is *cyberocracy*, from *cyber-* and *-cracy*, meaning authority. Actually it denotes 'rule' and refers

to interconnected computer networks. David Ronfeldt, an American political analyst, claims that although there is no *cyberocracy* in any of the countries of the world today, there are *cybercratic* elements, like violent treatment, especially in developed countries. A *cybercratic* government, a *Machine Rule* government, would quickly and effectively file 100% of its people plus any relevant foreigners, like refugees and immigrants.

Other *cyber-* formations that have appeared since the Seventies include *cyber law*, the area of law that deals with the relationship of the Internet to technological and electronic elements, including computers, software and hardware, and information systems. *Cyber law* prevents damage from *cybercriminal* activities by protecting information access, privacy, communications, intellectual property (IP) and freedom of speech related to the use of the Internet including websites, email, computers, cell phones, software and hardware, like data storage devices.

Cyber space or virtual reality developed to refer to the notional environment within which electronic communication (especially via the Internet) occurs. *Cyber space* remains the most popular cyber term used to refer to the world of electronic communications (including the Net). In the Eighties, there appeared compound words, like *cyber world*, *cyber land*, *cyber sphere* and *Cyberia* (from Siberia, i.e. *cyber-* + *-ia*, relating to punishment for *cyber criminals* or *cyber terrorists*) to denote the realm of information technology and electronic communication, especially the Internet. In addition, the combining form, meaning computer net work or virtual reality, used in the formation of compound words, like *cyber talk, cyber art* and *cyber fashion* is used to express strange visions of the future regarded as still to come.

The emergence of *e-* in compound words like *e-commerce* or *e-currency* changed things in the Nineties and Two Thousands. Influenced by the extensive use of *e-mail*, the letter *e-* assumed the place of *cyber* in the formation of technical words, replacing cyber formations. So, instead of websites, explaining the term *cyber commerce* Internet domains now discuss *e-commerce* and *e-currency*.

Despite the appearance of *e-* formations, terms like *cyber war, cyber attack, cyber crime, cyber terrorism* and *cyber bullying* are more prominent. This may be due to the clearer distinction offered by terms like *cyber war* against a formation like *e-war*, which is not quite clear. Newspaper articles on the 2014 hacking of Sony (subsequently connected to North Korea), the theft by *cyber crooks* of $1 billion from thirty different banks worldwide, and cases of bullying/harassment over digital devices and social networks strengthened the

importance of cyber terms, like *cyber cash*, *cyber economy*, *cyber buck*, *cyber dollar*, *cyber-money* and other terms that relate to *cyber-shopping*.

John Nagel, an American cyber security scientist, has counted more than a hundred words formed from *cyber-* during the last three decades. After *cyber space* in the early Eighties, *cyberpunk* appeared in the late Eighties to denote a subgenre of science fiction depicting life in the future and focusing on decadent life and advanced technological and scientific achievements, i.e. artificial intelligence and cybernetics put side by side with a social breakdown or radical change in the social order. The invention of cyber punk generated a great deal of derivative words, like *cyber-scribe*, *cyber-publisher* and *cyber-novelist*. When the Press became involved in the 'game' of inventing words related to electronic communication or its technology, there appeared terms, like *cyber-journalists*, who use *cyber libraries*, review *cyber thrillers* and write in *cyber zines* (short for magazines).

Scientists, writers and journalists continued to attach the prefix to science fiction characters, like "Doctor Cyber," a comics' super villain; "Cybermen," a fictional race of *cyborgs* who are the most persistent enemies of the hero of the British science fiction TV series *Doctor Who*; "Cyber Crime" or cyber investigations, as opposed to the forensic investigations, seen in *Crime Scene Investigation (CSI)*, the American police drama television series; the most persistent enemies of the British hero of the series; "Cyber Crime" or cyber investigations, as opposed to the forensic investigations, seen in *Crime Scene Investigation (CSI)*, the American police drama television series; and *Cyberchase*, a Canadian-American animated educational TV series that involves three children from Earth brought into Cyberspace, a digital universe, in order to protect the world from the villain Hacker by means of problem-solving skills in conjunction with basic Maths - in the presence of Digit, a *cybird* that they meet in cyberspace.

The film industry is not the only organized activity connected with contemporary arts. *Cyberformance*, from *cyber-* and *-formance*, from performance, has been coined to refer to live theatrical performances in which remote participants work together in real time through the medium of the Net, employing technologies like Chat applications. *Cyberformance* is also known as online performance and digital theatre. There is as yet no consensus on which term should be preferred although *cyberformance* has the advantage of compactness, as it is commonly employed by users of a special application to designate a special type of performance art activity taking place in a cyber-artistic environment. *Cyberformance* can be created and presented entirely online, for a distributed online audience that participates through internet-connected computers anywhere in the world. It can be presented to an

audience in a physical theatre or gallery venue with some or all of the performers appearing via the Net; or it can be a hybrid of the two approaches, with both remote and proximal audiences and/or performers.

In the United States, businessmen, influenced by the phenomenon of *cyber-mania*, have informed their customers that Black Friday is not the day to buy cheap toys for children. Shoppers should wait until *Cyber Monday* to get even better discounts. A toy company has even coined a new term *Cyber Week*, implying more discounts for toys throughout the week. What is more, entrepreneurs in Asia have established *cyber dhaba*, or roadside stalls, with computer facilities, where people can use the Net to search for information, send e-mails or engage in commercial transactions.

These interventions of contemporary science have created the term known as "virtual reality" or Internet fantasy ways of escaping from the stress of life and living in a world of cyberspace. Since the Eighties and Nineties the interventions have resulted in the increase of the number of cyber words from *cybernaut*, an expert or habitual user of the Internet, to *cyborg* and the new vocabulary mentioned above.

Besides programs that provide internet access, *cyber-* is used to refer to *cybercrime* or criminal activities carried out by means of computers or the Net. Cybercrimes are crimes in which computers are the objects of illegal acts, like hacking, phishing and spamming, and child pornography. *Cybercriminals* use computer technology to access personal information and business trade secrets. Using the Net for malicious purposes, they employ computers for communication, document and data storage. Criminals who perform cyber crimes, i.e. illegal activities, are often referred to as hackers. Common types of cybercrime include online bank information theft, identity theft, online predatory crimes and unauthorized computer access. When caught, cyber criminals hire *cyber lawyers* - experts on *cyber law* or the law relating to online communications and the implications of computers.

Serious crimes like *cyber terrorism* are now of great concern. Cyber terrorism is the use of the Net to conduct violent acts that result in political and/or ideological gains through intimidation and acts of deliberate disruption of computer networks by means of tools, like malicious software and hardware methods. *Cybercrime* comprises two categories.

- Crimes that aim at computer networks and devices, including viruses and denial-of-service (DoS) attacks.
- Crimes that aim at computer networks to advance criminal activities, like *cyber stalking* - the use of the Net to stalk an individual or organization in order to accuse them falsely

and defame them; offer sex for money; engage in identity theft and *phishing*, and the attempt to obtain sensitive information, like usernames, passwords and credit card details by disguising as someone trustworthy in an electronic communication.

Government organizations, in charge of Internet policing, aim at fighting cybercrime or searching for cybercrime fugitives who have committed bank fraud or devices that access personal electronic information. They investigate crimes including hacking or gaining unauthorized access to computer data and copyright infringement; issues related to confidential information lost or intercepted unlawfully; censorship, the suppression of published or broadcast material considered offensive or a threat to security, and propaganda or deceptive information that is widely spread. In India, for example, there exists an agency called *Cyber Crime Investigation Cell* whose major purpose is to fight computer crimes, enforce provisions of India's Information Technology or take measures to protect *cyber security*. In Greece, the Cyber Crime Department of the Hellenic Police, founded in the Nineties, was the conception of a Greek police officer trained by the United States Federal Bureau of Investigation (FBI). The officer started operations with the help of two more police officers. Nowadays, the unit is operated by at least eighty qualified law enforcement agents and civilians.

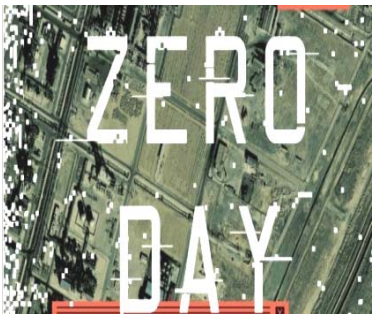
The importance of the work of government agencies, dealing with activities of the nature of groups engaged in *cybercrime*, cannot be exaggerated. Nor can government activities, handling *cyber attacks* and *cyber threats*, referred to as *cyber warfare*, like the targeting of computers, online control systems and networks, be overstressed. As cybercrime involves both offensive and defensive operations that are related to *cyber espionage,* countries like China, Iran, Israel, North Korea, Russia, the United Kingdom and the United States have developed *cyber capabilities* to engage in *cyber warfare*, both offensively and defensively in order to prevent cyber attacks against infrastructure; reduce national vulnerability; minimize damage and recovery time. To prevent the harmful effects of the new 'war' called *cyber warfare*, defensive measures have been established such as *Computer Security*, the security to computer parts, like computer hardware or the backup of the information stored in computers, and *cyber security*, the threats that can be caused in the Cyber Computer -

Online and Offline world, like viruses, stealing personal or sensitive government information.

To combat cybercrime and increase security, a number of *cyber countermeasures* have been established. It is defined as a system that serves to prevent the effects of a *cyber attack* against a computer, server or network. Recently there has been an increase in the number of international cyber attacks. In 2013, there was a 91% increase in cyber attacks and a 62% increase in security breaches. "The Convention on Cyber Crime and its Explanatory Report" (drawn by the Council of Europe in Strasbourg, France, with the participation of the Council of Europe's observer states (Canada, Japan, the Philippines, South Africa and the United States) was adopted by the Committee of Ministers of the Council of Europe in 2001 becoming active in 2004. So far sixty states have ratified the treaty, which deals with Internet and computer crime by harmonizing national laws, improved their techniques of investigation and increased cooperation. Russia has refused to adopt the treaty and cooperate in law enforcement investigations relating to cybercrime because she did not participate in the drafting. The "Additional Protocol to the Convention on Cybercrime" came into force in 2006. The countries that have ratified it are required to criminalize the dissemination of racist and xenophobic material through computer systems.

The effort to prevent *cyber warfare* or the use of digital attacks, like computer viruses and hacking by one country to disrupt the computer systems of another and create destruction, has increased. The reason is the attacks that have damaged enemy infrastructure, fighting alongside troops using conventional weapons, like guns and missiles. The combination of a cyber warfare arms race and absence of rules governing online conflict imply that there is a *cyber risk* that incidents may escalate. As contemporary societies rely more on computer systems linked to the internet, they become more vulnerable. If power stations, refineries, banks and air-traffic-control systems are attacked, people would lose their lives and property.

As with nuclear arms control, powerful countries need to consider how to restrict the threat of cyber war (or cyber attacks) before it is too late. Malicious computer programs, like Trojan horse, developed by hackers disguised as legitimate software in order to gain access to the systems of target users should be restrained. Users are tricked by attractive social media advertisements that direct them to malicious websites, loading Trojan horses on their systems. With the use of the malicious computer programs, cyber-criminals spy on the victim, gain illegal access to his/her system and extract sensitive data.



A *cyber crisis* occurred in Iran in 2010 when the country became the victim of a cyber-attack. A combined effort by the United States and Israel managed to infiltrate the country's nuclear facility. The infiltration was called 'Stuxnet,' a strong cyber weapon, referred to as *zero day*. A *cyber-worm*, Stuxnet damaged Tehran's atomic program and caused great delays. The Iranian government claims that it has discovered solutions to the worm and that its *cyber defence* is now better in terms of cyber warfare technology. So far, no *cyber activist* has claimed responsibility for the cybercrime.

Certain cybercrimes would have been avoided if the practice of *cyber hygiene* had been established. Cyber hygiene refers to the practice and steps that users of computers and other devices need to take to maintain system health and improve online security. The practice should become part of a routine to ensure the safety of identity and other details that could be stolen or corrupted. Like physical hygiene, cyber hygiene should be regularly conducted to keep away natural deterioration and common threats. The benefit of cyber hygiene, or having a routine cyber hygiene procedure in place for computers and software, is security.

Maintenance is necessary for computers and software to run efficiently, as files become fragmented and programs become outdated, increasing the risk of vulnerabilities. Routines include maintenance to spot problems and prevent them from occurring. A system that is well-maintained is less likely to be vulnerable to cyber security risks. Security is perhaps the most important reason to incorporate a cyber hygiene routine. Hackers, identity thieves, advanced viruses and intelligent malware are all part of a hostile environment. Because predicting threats can be difficult, preparing for them in order to prevent them is feasible with the appropriate cyber hygiene practices. All hardware programs like computers, phones or connected devices, software programs and online applications used, need maintenance, otherwise vulnerabilities, like loss of data, misplaced

data, security breach, out of date software and old security software, may lead to serious problems. Best practices to cyber hygiene include, among other things, password changes, back-up data and limiting users to their own data.

2 Conclusion

Concerning the future of our age of information, acknowledged experts on cyber policy and cybercrime, relate how cyber security has metamorphosed from an issue of limited interest to an issue of vital concern for national security, economic security and foreign policy. They relate the well-known international cyber security incidents, like the North Korean hacking of Sony Pictures and the Russian interference in democratic processes in America and Europe, to prove the truth of their argument. They claim that by combining information technology with diplomacy countries would experience a new more peaceful era, as *cyber diplomacy* or the evolution of public diplomacy would include and use the platforms of communication of the 21st century. As Professor Jan Melissen explains in his work *The New Public Diplomacy: Soft Power in International Relations*, cyber-diplomacy links the power of innovation in communication and information technology to diplomacy. Cyber-diplomacy is founded on the concept that new communication technologies offer new opportunities to interact with the public by adopting a network approach and making the most of an increasingly multi centric global and interdependent system. Cyber diplomacy, together with the rise of soft power in international relations, would request transnational collaboration to produce solutions to difficult problems. Thus, cyber diplomacy is more than a technical instrument of foreign policy. It is part of the changing of the nature of fundamental structure of international relations.

Both small and large countries, whether under democratic or authoritarian regimes, have recently displayed great interest in cyber diplomacy. Like cyber security, a technical issue that has economic and political dimensions and demands collaboration with professions to produce solutions to problems, cyber diplomacy requires collaboration among government agencies, organizations and industries. The establishment of an international cooperation would result in the establishment of *cyber norms* that would punish *cyber dissidents* for their behaviour. Yet, whereas the Western world shares information, Russia and China are among the countries that require absolute sovereignty in cyberspace. So, until the bridges between cyber diplomacy and the technical community have been built, people must remember that the Net is not operated by governments only but by the private sector as well. The Net is an international issue that different groups of people employ together. Christopher Painter, a State Department cyber coordination expert, claims that international

law should apply to cyberspace as law does to the physical world. There are a set of norms many countries agree to, like the idea that a nation should not attack infrastructures meant for the public good. Countries around the world need to adhere to these norms, he claims. This must be the role of diplomacy; the role of building alliances and showing international cooperation that would help a nation's diplomatic efforts to create an open, interoperable and reliable Internet.

References

[1] Crews, T.J. "What is the difference between computer security and cyber security?" <https://www.quora.com/What-is-the-difference-between-computer-security-and-cyber-security>.

[2] Cyber crime _ Counter measures. <https://en.wikipedia.org/wiki/Cybercrime_countermeasures>.

[3] Cyber-. <https://www.etymonline.com/word/cyber>.

[4] Cyber. <https://en.wikipedia.org/wiki/Cyber>.

[5] Cyber. <http://www.dictionary.com/browse/cyber>.

[6] Cyber Chase." *New York*, December 23, 1996.

[7] Cyber crime. <https://www.techopedia.com/definition/2387/cybercrime>.

[8] Cyberculture. <https://www.wordnik.com/words/cyberculture>.

[9] Cyber Diplomacy: New tools in the fight against hackers, attackers and other threats." <http://www.cornell.edu/video/cyber-diplomacy-new-tools-against-hackers-attackers>.

[10] Cyber diplomacy. <http://www.cornell.edu/video/cyber-diplomacy-new-tools-against-hackers-attackers>.

[11] Cyber Hygiene. <https://digitalguardian.com/blog/what-cyber-hygiene-definition-cyber-hygiene-benefits-best-practices-and-more>.

[12] Cyber is the New Black: Cyber Expert Points to Diplomacy to Solve Global Cyber Security Issues.” <https://cornellsun.com/2017/11/16/cyber-is-the-new-black-cyber-expert-points-to-diplomacy-to-solve-global-cybersecurity-issues/>.

[13] Cyber Monday. <https://www.msn.com/en-us/money/companies/wait-until-cyber-monday-to-buy-your-toy-gifts/ar>.

[14] Cyberocracy. <https://en.wikipedia.org/wiki/Cyberocracy>.

[15] Cyber party. <https://www.igi-global.com/dictionary/politically-oriented-database-applications/6568>.

[16] Cyber plague. <http://www.worldwidewords.org/articles/cyber.htm>.

[17] Cyber warfare. <https://en.wikipedia.org/wiki/Cyberwarfare>.

[18] Cyborg. Microsoft ® Encarta ® 2006. © 1993-2005 Microsoft Corporation. All rights reserved.

[19] Dhaba <Hindi. Microsoft® Encarta® 2006. © 1993-2005 Microsoft Corporation. All rights reserved.

[20] Melissen, Jan. <http://culturaldiplomacy.org/academy/pdf/research/books/soft_power/The_New_Public_Diplomacy.pdf>.

[21] Nagel, John. <https://www.linkedin.com/in/johngnagel>.

[22] Painter, Christopher. <https://cybersecforum.eu/en/speakers/christopher-painter/>.

[23] Ronfeldt, David. <http://wiki.p2pfoundation.net/David_Ronfeldt>.

[24] Trojan horse. <https://enterprise.comodo.com/what-is-a-trojan-virus.php>.

Elizabeth Hatziolou
Associate Professor
English Language and Literature
Hellenic Army Military Academy
Ηλ-ταχ.: savoula@otenet.gr

Stamatia Sofiou
Associate Professor
French Language and Literature
Hellenic Army Military Academy
Ηλ-ταχ.: dr.sofioustamatia@gmail.com