Web Journal of Current Legal Issues

Zekos, 'Globalisation and States' Cyber- Territory', [2011] 5 *Web JCLI*
http://webjcli.ncl.ac.uk/2011/issue5/zekos5.html

Globalisation and States' Cyber- Territory

Georgios I Zekos
BS(Econ), JD, LLM, PhD, Advocate and Economist
zekosg@yahoo.com , zekosg@uop.gr

Summary

Globalization is confronting the legality and the intelligibility of customary perceptions of territoriality. Cyberspace is the virtual space and place created by operation of any kind of interconnected electronic instruments producing a global virtual reality network accessible by different electronic devices currently from earth but why not from people out of space or virtual entities outside our space or of another dimension livelihood within our space without currently being traced by humans. The surface of electronic/cyber/virtual state sovereignty encloses the cyberspace territory and the state's authority to regulate and govern transactions taking place in cyberspace having effects upon the state's people living within the state sovereignty. Cyber state sovereignty should be the term for the entirety of international rights and duties that should be recognized by international law regarding this new dimension of the state's sovereignty. The depth of cyber state sovereignty is changeable without borders depending not only on the capacity of the used electronic technology in order to have access but also on the nature of the electronic networking which comprises the electronic/cyber state sovereignty.

Contents

Introduction

Globalization refers primarily to the progressive elimination of barriers to trade and investment and unprecedented international mobility of capital. Many of the functions traditionally performed by governments are being disaggregated and privatized. The Westphalian view was simple: each country was separated from its neighbors by frontiers: interaction took place at or across the frontiers. On a post-Westphalian view, there are no such separations: interactions take place within different "trans-national" networks. Moreover, globalization is confronting the legality and the intelligibility of customary perceptions of territoriality.

In today's technology-driven world, industry standardization, device interoperability and product-compatibility have turned out to be vital to advancing innovation and competition. Interoperability-centric challenges seem to continue to influence a variety of regulatory topics. Moreover, interoperability is one of the huge challenges of the convergence that occurs as a multi-level compatibility problem, purposely at the network, service, content and terminal equipment levels (Tambini et al, 2008). To attain interoperability and administer convergence-based complexities, the use of common standards and protocols, or the use of a conversion function to map between diverse services would be needed. Furthermore, the notion of interoperability, resting at the centre of network industries, is broader than merely a cyberspace entrée debate, as it influences innovation in software. The essential relationships among the components of the network, complementarity and compatibility, are present in many non-network industries, including financial intermediation and the exchange of financial instruments and assets. Complementarity requires compatibility and coordination

Cyberspace is already a global communications medium and the subject of valid international interest (Johnson-Laird). Internet takes the user to the separate place of cyberspace and no one exists in cyberspace without an Internet account. Cyberspace life exists only as long as somebody is logged on to Internet and the act of turning off the computer removes somebody from cyberspace.

A domain name is a significant part of an Internet address that determines where data packets are to be sent (*ACLU v Reno* 929 Fsup 824, Zekos, 2003, 56-79). Domain names do not effectively reside in a physical location and the efficacy of the domain system requires expansion beyond territorial boundaries and into globally integrated laws. An effective domain name system will function properly from both a technological and management standpoint. The entity in a position to dictate the content of these network protocols is a primary 'rule-maker' in regard to behavior on the network. Each network has its own message origination and routing rules. Moreover, communication networks are defined at a minimum by a set of rules specifying the medium through which messages can travel and the characteristics of the messages that are permitted to enter the network. Therefore, the electronic market itself regulates Internet. Rules concerning "due process" for users can be efficiently

adopted by consensus, so long as a "standard" or "protocol" is a required condition for connection or for inclusion in the groups collaborating to improve the functionality of online communications. The key feature of the Internet is that the net is set up to operate logically rather than geographically.

This author considers that cyberspace is an electronic place that conforms to our understanding of the real world, with private spaces such as websites, email servers, and fileservers, connected by the public thoroughfares of the network connections. Moreover, Cyberspace is the virtual space and place created by operation of the Internet (*Voyeur Dorm v. City of Tampa*, 265 F.3d 1232), a network of computers that share information with each other, and any other electronic networking resulted by different electronic devices such as satellites and cellar phones that can be interconnected and producing a global virtual reality network accessible by different electronic devices currently from earth but why not from people out of space or virtual entities outside our space or of another dimension livelihood within our space without currently being traced by humans. It has to be taken into consideration that virtual events can be understood by human beings as human beings by the use of electronic devices transforming electronic signals into words and pictures viewed and comprehended by human beings and not virtual ones.

"Sovereignty" is an adaptable perception. The term "sovereignty" has a range of meanings and in its widespread modern treatment, sovereignty is the term for the "totality of international rights and duties recognized by international law" (Crawford, 1979, 26-27) as residing in an autonomous territorial unit, the State. A sovereign nation state is an entity whose sovereignty jointly derives from the sole jurisdiction to make laws for its people and its freedom from the coercive authority of any other state (Gilson, 1984). Moreover, the state lies upon the foundation of sovereignty, which expresses internally in the supremacy of the governmental institutions and externally as the supremacy of the state as a legal person (Masilamani and Anup Kurvilla, 2001). The courts derive its power to adjudicate a matter from the state. Therefore, the concept of jurisdiction is based on the concept of state.

The Jurisdictional bases are the following*:* first *territoriality*; under the principle of territoriality, jurisdiction is based on acts that have been executed within the territory of the State in question. An alternative of this is the 'objective territoriality principle', purporting that the function in question was begun abroad but concluded within the territory of the State, or that a constitutive part of the conduct happened within the territory (Michaels, 2004, 106). Second *personality*: under the principle of personality, jurisdiction is upheld by the State of nationality of the perpetrator (active personality principle) or of the victim (passive personality principle) (Cafritz and Tene, 2002-2003, 588). A number of countries confine passive personality jurisdiction to the cruelest of crimes, such as terrorist hijackings and crimes against humanity. Third *effects doctrine*: the 'effects doctrine' jurisdiction is established on the fact that conduct outside a State has effects within the State but it is open-ended, given that in a globalized economy, everything has a consequence on everything (Schultz, 2008, 815). All countries have a connection to all websites by virtue of their accessibility. Should the 'effects doctrine' *a fortiori* be rejected completely on cyberspace? The divergence between the objective territoriality principle and the effects doctrine is vanishing because of cyberspace, given that the act of letting a message or information be seen in another territory and the effect caused by it are tricky to

differentiate (Hayashi, 2007, 74-75). Fourth *protective principle*: The protective principle is considered to protect a State from acts performed abroad that put at risk its sovereignty.

The territorial jurisdiction of states and the jurisdictional limits of the municipal courts are established on the territorial theory. Personal jurisdiction depends upon some quality attaching to the person involved in a particular legal situation which justifies a state or states in exercising jurisdiction in regard to him/her. Personal jurisdiction may be exercised on the basis of one or other of the following principles: (a) active nationality principle: Under this principle, jurisdiction is assumed by the state of which the person, against whom the proceedings are taken, is a national and (b) passive nationality principle: Jurisdiction is assumed by the state of which the person suffering injury or a civil damage is a national. It has to be taken into account that it has not been established an effective or recognized customary international law that controls personal jurisdiction (Goldsmith 1998).

Taking into consideration the characteristics and impact of globalization, we investigate the emergence or not of universal cyber-sovereignty and cyber-territory of a state and consequently identifying the potential impact upon the traditional state sovereignty/territory. The impact of globalization upon law and economy is discussed firstly. Secondly there is a specification of the nature of cyberspace in order to understand the character of the electronic environment. Thirdly we point out the control or not of cyberspace by states. Fourthly there is a presentation of the traditional notion of sovereignty before the analysis of the cyber sovereignty/territory. The analysis of the traditional understanding of sovereignty allows us to see the comparatively new that emerges due to the development of cyber sovereignty/territory which influences the legal and economic status quo in a society. Finally, our conclusions bring forward a likely new status caused by the emergence of electronic/cyber/virtual state sovereignty in a globalized environment challenging the ability of current legal systems to regulate it successfully.

Globalization

Globalization, as a process, is by now a historical fact, which enriches the interactions of people in a lot of different countries: they meet, swap goods and ideas and borrow or buy resources. Globalization, in economic terms, can be thought of as a process in which business decisions, production processes and markets gradually come to exhibit more “global” characteristics and less “national” ones. The current process of globalization is shifting the balance from the internal to the external market.

Globalization is associated primarily with the industrialized countries of the Triad (Europe, North America and Japan) and its effects diverge across industries and are predominantly acute in sectors, which are capital and knowledge intensive, as well as those that depend on new and fast-evolving technologies. Alongside the new opportunities in trade and external finance offered by globalization have come new challenges of economic management in an ever more open, integrated, and competitive global economy. Public policies have significantly influenced the character and pace of economic integration, although not always in the direction of increasing economic integration.

The procedure of globalization along with liberalization and privatization has been introduced with a view to integrate the world economy in order to cause faster movement of factors of production. There is an increase of world trade cutting down the transport expenditure and stepping-up technology from one region to another adding to the growth procedure of different countries worldwide.

In the globalization phase particularly after 1990, the international mobility of capital, resulting from progresses in technology field and liberalization of financial markets has intensified as the world economy witnesses the relinquishing of market forces. There is deregulation of domestic markets opening them to competition and privatization. The consolidative philosophy of globalization appears unappeasable and its impulse is overwhelming.

Legal actors are more and more caught in a concurrent direction toward globalization and privatization impelling them to take on a fast increasing plurality of legal regimes. The way toward globalization moves the center of gravity of the legal order from the conventional Westphalian nation-state to the supra-national or even the global domain. The integrity and hierarchy of legal norms imposed by the constitution representative of the Westphalian nation-state tends to unravel, leaving legal actors at the mercy of conflicting and at times even contradictory legal responsibilities rooting from incompatible sources of law (Rosenfeld, 2008; Kelsen, 1961, 124). Moreover, the total legal system of the Westphalian nation-state is integrated and subject to constitutional and democratic restraints. Consequently, any transfer away from that legal system to a supra-national one inclines identical issues of legitimacy.

Through privatization, legal actors can get away from the restraints of law coming from the nation-state and once public functions subject to criteria of accountability and transparency can be handed to non-governmental actors availing themselves most of the profits of those who maneuver within the private field.

Supra-national legal regimes do work and can, as the WTO, the ICC and the EU most notably do, achieve a high level of legal legitimacy (Lindseth, 2010, 7; Fassbender, 1998, 529). Furthermore, even international regimes with acknowledged global ambit are credibly understood as comprising legitimate legal regimes.

Privatization constitutes two distinguishable phenomena: privatization of an applicable legal regime as in the switch from a nation-state's commercial law to *lex mercatoria* regulating business dealings among MNEs; and privatization of a conventional governmental affair by "outsourcing it" to a private entity, such as substituting a state run police force by one controlled by a private security company. Furthermore, there can be many transfers of power going from the public domain to the private one that do not imply privatization but producing effects that are mostly functionally equivalent.

Globalization is in principle totally indifferent as between public or private law. Accordingly, the fundamental modifications brought about by globalization and privatization and by the consequent development of legal pluralism and the spread of supra-national and privatized layered and segmented legal regimes presents a series of tough new problems, but does not, at least in the first instance, necessitate a

replacement of constitutional ordering by its administrative counterpart or for a redrawing of the public/private divide.

What kind of space cyberspace "is"?

Cyberspace is profoundly and fundamentally different from "real space" (*Reno v. ACLU*, 521 U.S. 844). The Internet is purely a communications network part of a further electronic circle called cyberspace. It has to be taken into account that the concept of cyberspace consists of three levels. The physical level is comprised of material objects such as wires, mobile phones, satellites, computers and wires liking computers. The logical level consists of open protocols governing the exchange of data across the network. The content level is the digital data itself which is easy to access, copy, exchange and distribute.

Moreover, cyberspace is viewed by real users who feel cyberspace and real space as different but connected, with acts taken in one having consequences in the other. There is an intricate interplay between real-space geographies of authority and their cyberspace equivalents (Johnson, 2004). Therefore, cyberspace is a space separate from real space and not purely a continuation of it. Additionally, cyberspace and real space co-exist as being spaces of a different dimension and the one resides inside the other (Cohen, 2000, 1377-91).

Furthermore, cyberspace users are situated in both spaces at once because of the humans' ability to exist as human beings and to think as spiritual creatures. The ability of humans via the technology to perceive virtual-reality and being at the same time humans is intriguing but the moment that the human perceives virtual-reality does not notice the human moment but the human being recognizes it as a human being. The human being as a simple user of cyberspace is merely one person who uses technology to learn or express himself/herself as a spiritual human being.

The possibility of signals to travel through wires or wireless pre-exists and the humans simply discover or invent the apparatus making possible the transfer of signals. Who knows or can deny the fact that the human spirit as a spirit can travel in cyberspace and understand more advanced type of electronic signals in cyberspace rather that the human being made by material suitable only for a materialistic world? Thus, cyberspace as phenomenon of signals able to circulate electronically in an electronic system pre-exists its users. The information circulated in cyberspace is created by its users. The incapacity of humans to understand other dimensions or information circulated in signals of other dimension does not mean that they are not in existence. The spiritual world is another world and humans have got the ability to sense and live this world of course by remaining humans not mentioning the capacities of the human spirit as a spirit when the spirit leaves the body. Dreams are an example of the dimension and power of the human spirit as spirit. Humans as long as remain humans cannot be transformed into electronic beings. Bodies continue existing in the space of the world but the spirit imprisoned in the body can sense and reside in a spiritual world.

The technologies and virtual places that represent cyberspace have been assimilated into the lives of people who accept the Internet as a tool for pursuing their common, real-world needs. The information circulated in cyberspace produced by real people.

People can use cyberspace framework only for their online dealings (Bradley and Froomkin, 2004, 139-146). Other people can use cyberspace setting for free circulation of ideas or having the impression of travelling virtually in many other places (Castronova, 2004, 200-205). Even why not if it is made possible, in the distant future, to achieve interconnection with digital networks of other civilisations living out there in space.

Courts are using the metaphor of cyberspace as a "place" to justify application of traditional laws governing real property to this new medium (*eBay, Inc. v. Bidder's Edge, Inc*., 100 F. Supp. 2d 1058). It should be taken into account that the Internet is not "just like" the physical world. Not every Web site is necessarily a purposeful attempt to avail the benefits of every forum state (Litman, 1999, 1725). Furthermore, the courts showed significant keenness to treat Internet and paper transactions as equals; comparable results should be reached if not there is a reason to treat them in a different way (*CSX Transportation, Inc. v. Recovery Express*, Inc. 415 F. Supp. 2d 6). For instance, a contract cannot be denied enforcement solely because it is in electronic from or signed electronically ("UETA", 7A U.L.A.§701, "E-Sign", 15 U.S.C. §§7001-7031). On the Internet, problems of physical infrastructure and overcrowding are less apparent because is a different dimension (*Intel Corp. v. Hamid*i, 114 Cal. Rptr. 2d 244) but it has to be taken into account that electronic infrastructure used to accommodate the operability of cyberspace causes very often many problems due to its material feature. Moreover, information is saved in electronic devices and is not freely circulated on earth like sound, wind or oxygen and so controlled by the owners of the electronic devices.

Information companies desire that information technologies should be redesigned to build in control via digital rights management. Cyberspace allows the implementation of different activities such as online gaming, online banking, fan fiction, comparison shopping. In fact, cyberspace brings forward a question of allocation of rights and responsibilities in virtual space. What occurs in cyberspace is related with what occurs in real space. People are using cyberspace and circulate information or contact electronic transactions. Information access and control in cyberspace have consequences that reflect into real space because it is people in real space who require information residing in different jurisdictions (*Reno v. ACLU*, 521 U.S. 844; Lemley, 2003; Agre, 1998). Thus, lives and concerns of people using cyberspace are inextricably rooted in real space.

Space encompasses geographic/mapped places representing both totality and infinity. To that extent cyberspace as a virtual space encompasses virtual places with a virtual totality and infinity and the countless amount of virtual places constitutes the cyber place of cyberspace. Hence, cyberspace includes many cyber places. Moreover, cyberspace is a separate space in a virtual dimension viewed and operated by electronic agents programmed by humans. It is necessary to be made the distinction between cyberspace as the place and space where different type of virtual activities can take place that have an effect on humans and cyberspace as a virtual place and space where virtual functions can take place which are only virtual without affecting humans. Cyberspace as a virtual space and place can be used by virtual entities and electronic beings but presently human being do not have this ability to be transformed from human being into electronic beings and vice versa. The future use of cyberspace –not merely Internet- by virtual entities and electronic beings to inflict the real world

cannot be overruled in advance which will cause different problems giving a different dimension into the phenomenon of cyberspace needing a state's intervention. The production of electronic beings that will function only electronically on behalf of human beings cannot be rejected for the distant future. It is open to research if cyberspace in its current form or a new more advanced cyberspace based on wireless communication can be connected with unknown electronic/digital systems own by civilizations out of our planet but within the endless cyberspace.

Cyberspace is not a real place and so users can adopt a new electronic identity with which travel in cyberspace. The electronic user always will correspond to a real person who can adopt many different electronic identities as technical identities allowing him/her to use cyberspace not mentioning purely electronic agents that can be used in electronic transactions. Electronic agents will continue to remain electronic agents created by humans to act as electronic agents having no liability. On the other hand, humans even as electronic users have finally liability for any misgivings caused by their electronic transactions.

State's Control Over Cyberspace

Cyberspace was initiated by the State, and soon after was privatized and so the State minimized its straight connection in the information environment and more and more abandoned its role in running the Internet but not cyberspace and electronic networking in a broad sense. At the beginning the Internet was considered to be an international innovation lying beyond the reach of laws (Marrella and Yoo) of any specific government (Netanel, 2000). On the other hand, the advance of cyberspace has challenged the law as new technologies characteristically do and the dilemma is whether to modify old legal doctrines in order to deal more effectively with the new reality or to acquire expressly tailored new doctrines (*In re C.K.G.*, 173 S.W.3d 714, 730-32). It has to be taken into account that inventiveness does not forgive cyberspace technologies from conformity with the law (*Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 167). Thus, cyberspace is still not above the law, whether on an international or community level (*Commonwealth v. 141 Internet Domain Names*, No. 08-CI-1409).

Cyberspace is a network, which grew, suddenly, into a global network of networks, challenging the State's capacity to govern. It is vital for states to control the distribution of information. States affect the information surroundings in one of two roles: as a participant, exercising its power through its agents to perform state action, or as a regulator, establishing a legal order or a system of rules, all the way through the legislatures and the courts. Moreover, States have a responsibility to safeguard their citizens from all forms of harm, whether digital or analog. Thus, Governments maintain ownership over information exchange systems so as to preserve their control over ways of exchanging and disseminating information. To that extent, the digital/electronic environment makes possible the establishment of monopolies that gain their monopoly status by controlling technological standards (Elkin-Koren and Salzberger, 1999, 557-559; *Sun Microsystems Inc. v. Microsoft Corp*., 240 F. Supp 2d 460).

During the first steps of cyberspace, its global and digital nature appeared to marginalize the state by weakening the legitimacy of State regulation that would

typically be justifiable within territorial borders. Thus, the cross-border character of cyberspace has caused problems regarding the enforceability of laws imposed by the State, in this manner further weakening the effectiveness of State regulation. Moreover, technological change has weakened the efficacy of State regulation, making it almost unfeasible for regulators to keep up with a technology that reinvents itself constantly. The majority of states use output access providers for filtering or blocking cyberspace content on its way to the end user. Search engines have develop into significant players in the information age. Furthermore, the search engine provides copies of the indexed sites that permit users to see content of the site even if the site itself is blocked.

Multinational enterprises (MNEs) in the electronic industry turn out to be highly mobile and independent of any specific location (Zekos, 2008a, 2007a, 90). The capacity to convey information and knowledge effortlessly allowed MNEs to organize themselves across national borders, in so doing decreasing the governance of the State in organizing economic activity. Thus, the design and codification of digital technology allowed private companies with regulatory power in shaping the information environment.

The State as a regulator constitutes a system of rules producing rules, intended to resolve conflicting interests, aiming at protecting rights or advancing policy objects through the legal system (*Hughes v. Alexandria Scrap Corp*. 426 U.S. 794; *Reeves, Inc. v. Stake* 447 U.S. 429). Accordingly, Regulations shape the information field openly, defining what is right or what is wrong in online behaviour, or ultimately, by establishing the legal infrastructure of online markets, subsequently enabling states to take control. Therefore, direct regulation is most apparent in the effort to control the distribution of content that is perceived to be harmful.

The State becomes an active player, taking action in the online setting to secure national interests in a global network. The State no longer restricts itself to the role of a neutral regulator, a forum for resolving conflicting welfare and ideologies of its population through a system of rules; rather, it employs its ancient duty of securing individual safety and national security. Therefore, the digital setting (cyberspace and electronic networking) is perceived as threatening national security and as a field that has to be governed. In other words, the digital setting creates another electronic sovereignty needing to be governed and safeguarded.

To avoid illegal content from getting online, a state can set up civil and criminal sanctions on the input user. Owners of electronic technology at the utmost level might be able to intrude into every electronic communication and so they can control everything. A state may only successfully impose the rules to those users who reside on the state's territory. Even though international law recognizes the power of a state to impose laws to foreign actors under particular circumstances, the authority to implement the laws often works as a practical constraint on it.

Cyberspace promoted online sales of weapons and ammunition, and the availability of technologies or information become useful for mass destruction. Moreover, cyberspace conceived as one of a few means of communications that can be used by terrorists, as well as other cyber-criminals (Etzioni, 2002, 257) and so it is a territory of interest to the State’s numerous security agencies. Furthermore, cyberspace offers

devious people a completely new scene in which to conduct harmful activities without a considerable chance of being identified. Thus, cyberspace enhanced its misuse as an instrument of crime - either as a means in the performance of "traditional" crimes, such as using a telephone to coordinate a crime or to conduct commonly referred to as "cybercrime" (Convention on Cybercrime, Nov. 23, 2001 ; Yeates, 2001, 131-134). The new technology's distinctive characteristics, such as its non-territorial and decentralized architecture, have raised new challenges to law enforcement around the globe.

Cyberspace activity allows State intervention just as any other human activity that could affect public welfare (Barrett, 2002, 16; *U.S. v. Scarfo*, 180 F. Supp. 2d 572). The analysis shows that states assumed control over cyberspace regardless of any philosophical views, approaches and writings for its nature and character and for a free cyberspace (Zittrain, 2003; Boyle, 1997, 178). Therefore, states have already imposed authority upon this new electronic territory as part of their state sovereignty and so configuring their new electronic state sovereignty.

State sovereignty

Sovereignty is not itself a prerogative nor is it a principle for statehood (Shinoda, 2000, 1). Moreover, sovereignty implies a state's legal monitor over its territory commonly to the exclusion of other states, power to govern in that territory, and power to enforce law there (Woolsey, 1883). Sovereignty, while its meanings have varied, also has a main meaning, supreme authority within a territory. Thus, the sovereign's power over people is supreme. Characteristically, authority derives from a body of law, a constitution, inherited succession, or even divine mandate trigger both this presupposition of supremacy and the recognition of it by those who are governed (Sunstein, 2001, 241). International law permits a definite liberty of the states on the issue of jurisdictional order (*S.S. Lotus (Fr. v. Turk.)*, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7); Reydams, 2003).

Sovereignty resides in that political body known as the state amd so Sovereignty is a quality of statehood (Hannum, 1990). Internal political ordering is an underlying feature of state sovereignty (*Gregory v. Ashcroft* 501 U.S. 452, 460 (1991)) and the legitimacy of a specific exercise of political power is a question of legality.

Signals of the independence of a state's sovereignty are: the exclusiveness of power over its territory and citizens, execution of foreign policy, deciding on engaging in war or retaining peace, free recognition of states and governments, decisions concerning the creation of diplomatic relations, participation in military alliances and in international organization (Dinh, 1999). A state is a formal imperative (*Fed. Mar. Comm'n v. S.C. State Ports Auth.*, 535 U.S. 743). Moreover, a state has authority to regulate the transmittal of information across its borders and the use of that information by individuals within its territory (Wilske and Schiller, 1997, 129-142; Goldsmith, 1998a). States rely on the territoriality principle to regulate in-state hardware and software used in Internet communications. Moreover, state control is fundamental of state sovereignty (*Nixon v. Missouri Municipal League*. 541 U.S. 125).

The perception of state sovereignty has an external and internal substance, and they are equally constitutive and reinforcing: externally, a sovereign state is recognised as an independent body at international law; internally, a sovereign state exercises supreme municipal authority. States cannot intrude in one another's affairs by force without authorization from the Security Council (U.N. Charter art. 2). Is the sovereignty of the Great Powers somehow different from that of less equal states? As Brownlie notes, "the sovereignty and equality of states represent the basic constitutional doctrine of the law of nations." (Brownlie, 1999, 289) The Great Powers cooperatively drive globalization from which they also excessively benefit. The club of Great Powers is not immobile. Who determines which state poses a threat over the world and under which criteria? Which is the principle that can be used in determining the actions of a state considered to be a treat that it poses against the world? It is obvious that divergence among states occurs on the severity of and urgency for addressing threats or the means to be used (Bajema and Nikitin, 2004, 163). On the one hand, the legitimacy of international law is a question of state participation and endorsement. It is the state's sovereign authority to legislate that makes possible the juridical recognition. On the other hand, the Great Powers also control decision-making and policy-making all the way through their majority share voting rights at the World Bank and the IMF which accords them more shares based on their larger economies.

The present states' security is defined in terms of its rights and control over specific territory (Wendt, 1992, 414). Territorialism is the practice of states exercising exclusive jurisdiction over assets and parties within their borders. Can this specific territory be extended to enclose an electronic state territory? The analysis shows that the state has taken control of cyberspace transactions having effects upon its people and so it considers cyber- territory as part of its own territory. On the one hand, cyberspace and electronic networking can be seen as a post-national situation (Johnson and Post, 1996) On the other hand, states are not expected to decline in importance in the information age (May, 2002)

Even though the perception of sovereignty assigns to the state supreme political authority within a bordered territory, the scope and substance of this "authority" are defined and legitimated by global cultural processes (Goodman and Jinks). The development of cyberspace as an electronic networking in a broad sense changes the character of sovereignty. Globally-legitimated concepts of sovereignty not only authorize, but also hamper the "legitimate actor-hood" of states. Sovereignty and the integrity of the state can endorse extended internal armed conflicts. Appeals to sovereignty threaten constitutional norms and protections (*United States ex rel. Knauff v. Shaughnessy*, 338 U.S. 537).

Electronic activity occurs across multiple jurisdictional boundaries which means that the effects of online activities are not tied to geographic locations but can be felt by people living in a specific place (Boyle, 1997; Reidenberg, 1996, 917-919; Wu, 1997, 654-655). In addition, globalisation and the development of cyberspace add to the alteration of decision making authority in international organisations and so further alteration of national sovereignty in the traditional meaning and sense (Flaming, 1997, 179).

Application of Law upon the Surfaced State's Cyber-Territory/Sovereignty

Cyberspace is growing at a tempo that outpaces any modern medium of communication. As presently organized, cyberspace depends upon a fixed technical infrastructure. The informational activities in cyberspace result from the generation, storage, and transmission of personal data in personal computers, Internet Service Providers (ISPs) and, Web sites. Thus, the Internet's technical virtues have a negative outcome by making achievable an intense surveillance of activities in cyberspace (Conrad, 2001). To that extent, companies now engage in a continuous collection and analysis of personal data from cyberspace to permit the customization of products, and services (Gates, 1999, xiv; Elkin-Koren, 2001, 171)

Cyberspace allows users to view a practically unlimited number of files that display text, images and sound. Therefore, an unregulated cyberspace has intrinsic characteristics that support unlimited economic opportunity, equality, party freedom, and even political liberty (Post, 1998, 539). Furthermore, cyberspace enables a mixture of human activities, all of them amazingly diverse from each other in their social and legal meaning. To that extent the state has to ensure that rules and principles developed for the real world do not lose their importance in the digital word. As mentioned earlier a specific activity cannot escape regulation just because it is committed by means of the global computer network. On the other hand, no state can regulate all human activities in all parts of the world but the concept of territoriality has not lost its meaning in the digital epoch.

Is cyberspace territorial? Cyberspace is characterized as "a-territorial" (Rosenne, 2003, 349) with the conventional understanding of territory but cyberspace creates the notion of cyber-territory.Taking into account that many types of activities take place in cyberspace affecting people in real space cyberspace can be used in practice as a tool for hegemonic exercise of control. So, the effects of actions that take in cyberspace are evidently perceptible within the territory of each state that might want to regulate that action.

Do changes catalyzed by cyberspace in real world and space make cyberspace different? Does cyberspace change real space? Cyberspace includes a range of places connected to real space in many different ways. A communications network changes the character of existing space. Thus, changes in the ways that information is experienced and the ways that economic, political, and personal dealings are structured change the nature of real space. Moreover, Internet activity corresponds substantially to the real-world organization and attributes to the economic activity but this does not define its characters but its usage. Technology is not void of values but also it can be used as the means for the communication of values. Hence, technology not only affects new values but also assumes, reflects, and serves these values. Cyberspace as the key mean of communication and trading produces uninvited "political and ideological consequences" (Burk, 2003, 17 and 18). Hence, cyberspace as presented above changes the face of state sovereignty by introducing the notion of the cyber-sovereignty of a state and so expanding the whole state sovereignty as analysed earlier. In other words from boundary territorial state sovereign we have come across a un-boundary a-territorial cyberspace state sovereign.

Is cyberspace a separate jurisdiction, in which the laws of real space need not to apply? Connectivity on national and global scales is pervasively remaking the model of experienced connections. Global connectivity promotes personalized trade and electronic commerce. Electronic commerce conducted through cyberspace brings forward a weakening of territorial borders and so there is a need for increased emphasis upon not only national but also the international aspects of law. In fact, cyberspace disrupts existing power relationships and enables new ones. On the other hand, the market, norms, law, architecture (Almog, 2002, 3) and their interactions regulate cyberspace (Lessig, 1996, 883-895; Benkler, 2000, 562-563). Global space is produced by the interconnectivity of cyberspace over "real" space, and by the interpenetration of the two which means that cyberspace extends further than the boundaries of any of the states, and the effects of any individual state regulation similarly spills over that state's borders (Berman, 2002, 321-322) As a result the extensive availability of cyberspace has changed the character of commerce and communication.

On the one hand, cyberspace cut across territorial borders, creating a new land of human activity and undermining the practicability and legitimacy of applying laws based on geographic borders. On the other hand, all law is prima facie territorial (*American Banana Co v United Fruit Co* 213 US 347). If sovereignty defined as the "final authority within a given territory", (Krasner, 1988) then the escalation of internalisation via cyberspace transactions will have supplementary important implications for State sovereignty. Existing international laws are predicated on the being of the sovereign State and the conceptions of sovereignty and statehood were among the central aspects of public international law. Sovereign states enjoyed almost unfettered independence of action and the legislative jurisdiction of a State is limited to its territory. Location is central, but it is virtual location, rather than physical location and there is no indispensable connection between a cyberspace address and a physical location. Thus, there is a need the conception of sovereignty to be interpreted by international law in a way that it includes the notion of electronic state sovereignty as well.

The execution of jurisdictional competences is above all a territorial phenomenon and State competences come to life in a precise space in a conventional understanding rather than a totally virtual space and remain bound exclusively thereto but space is surrounded by a virtual one perceived only and solely by virtual beings and by humans as well given that the virtual signals are transformed into signals perceived by humans. Moreover, the state is competent to embark on jurisdictional activities with respect to events happening abroad, but resulting within the state territory. Already, states have begun asserting their jurisdiction outside their own territory with regard to conduct on cyberspace, to the point where this has become the rule rather than the exception (Svantesson, 2007, 1). Under the principle of territoriality, jurisdiction is based on acts that have been committed within the territory of the State in question and correspondingly any acts have committed on cyberspace territory energize the electronic jurisdiction of a state (Ryngaert, 2008, 187).

The boundaries of cyberspace are continuously being re-determined but boundaries do exist in a sense that the boundaries are shaped according to the capacity of the whole network of utilized electronic devices that materialize cyberspace as an electronic system. The surface of electronic/cyber/virtual state sovereignty encloses the

cyberspace territory and the state's authority to regulate and govern transactions taking place in cyberspace having effects upon the state's people living within the state sovereignty as analysed above. Thus, electronic state sovereignty implies a state's legal monitor over its electronic territory commonly to the exclusion of other states, power to govern in that electronic territory, and power to enforce law considering electronic transactions affecting state's sovereignty. As mentioned earlier, the boundaries of an electronic/cyber/virtual state sovereignty are not fixed but they are flexible depending on the capacity of the technology and accessibility taking into account that the point of accessibility has to be located within the traditional state territory. Satellites or space stations should be considered as state territory. Electronic/ cyber/virtual state sovereignties are overlapping and there is a danger easily to have intrusion into electronic states sovereignty since electronic transactions can have simultaneously effects upon many jurisdictions.

In the real world the concepts of sovereignty and territoriality played and continue to play a significant role, defining not only the state power but also the limits of this power and contributing to peaceful coexistence of various states and cultures. As a result states' authority correspondingly should continue in cyberspace sovereignty and territoriality comprising the electronic state sovereignty. To that extent, the Westphalian system of international law among sovereign states considered international law as mutual restrictions on state power aimed at protecting international order. Conventional principles of international law such as sovereign equality of states, non-intervention into national affairs are more and more qualified in the law of global and regional organizations. Therefore, those principles of sovereign equality of states, non-intervention into national affairs could and should be applicable to cyberspace territory and sovereignty comprising the electronic state sovereignty.

Cyberspace is causing a crisis in application of the territoriality principle, as long as it can be nearly impossible to localize an act of data processing as taking place in an individual State (Michaels, 2004). Moreover, cyberspace drastically destabilizes the relationship between legally considerable electronic/digital phenomena and physical location (*United States v. Am. Library Ass'n*, 123 S. Ct. 2297). The development of the electronic networking is destroying the connection between real world location and the authority of a local sovereign's efforts to regulate electronic global phenomena. Electronic/digital activities that even modestly affect the critical interests of sovereigns are becoming subject of regulation by sovereigns (Goldsmith, 1998b; *Reno v. ACLU*, 521 U.S. 844). Only purely electronic/digital activities affecting merely cyberspace could be considered as matters suitable for self-regulating structures of cyberspace.

Cyberspace regulation cannot be a regime independent of national laws. Infringement to space/place in cyberspace is alike to infringement to chattels in the real space for the reason that space in cyberspace is just real-space chattel, the server. It is space on the server that is being used without permission causing impairment to who owns the server and websites (*Intel Corp. v. Hamidi*, 71 P.3d 296). Illegal visitors of websites are deemed trespassers because they are entering websites using the store without authorization, and this behaviour causes damage to the chattel in the sense that limited and precious "space" is used illegally(*eBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058; *Oyster Software, Inc. v. Forms Processing, Inc*., No. C00-0724 JCS, 2001

WL 1736382). We should deal with trespassing on business premises the same, whether the trespass occurs in cyberspace or real space as long as both have an impact upon people living in the real world (McGowan, 2003, 353-358; *Am. Online, Inc. v. LCGM, Inc*., 46 F. Supp. 2d 444; *Register.com, Inc. v. Verio, Inc*., 126 F. Supp. 2d 238).

While public international law only applies solidly to relations between States, its function as the key limiting standard of the international legal order presents the testing ground for jurisdictional rules involving private parties in different States as well. When an actor places information on the cyberspace, he/she can communicate with persons in almost every jurisdiction. It is worth mentioning that people placing information on the cyberspace has to be subject to personal jurisdiction in every State which has suffered any consequences due to the placed information. However, state judicial power over persons remain limited to persons within the State's borders and to those persons outside of the State who have least contacts with the State such that the State's exercise of judicial authority over the person would not offend traditional concept of fair play and substantial justice. *Zippo Manufacturing Company v. Zippo Dot Com (*952 F. Supp. 1119; *Metcalf v. Lawson*, 802 A.2d 1221; *Karstetter v. Voss*, 2006 WL 279377) is the key case that formulated the framework now used in the determination of personal jurisdiction in cyberspace cases (Zekos, 2006; *Richard Freer, United States v. Swiss Am. Bank, Ltd*. 274 F.3d 610).

Modern geolocation technologies permit cyberspace sites to automatically and correctly spot a user‘s geographic location. To that extent courts and regulatory agencies have considered cyberspace not as some sort of special place and consequently, cyberspace is becoming less independent and more geographically delimited. It has to be taken into consideration that laws diverge significantly from one jurisdiction to the other, such that content or services may be legal in one jurisdiction and illegal in another creating a great demand for sophisticated geolocation technologies that can correctly and automatically screen users by jurisdiction allowing online traders to do as much dealing as achievable without breaking the law. The *Zippo (Zippo Mfg. Co. v. Zippo Dot Com, Inc* 952 F. Supp. 1119, *Best Van Lines, Inc. v. Walker*, 490 F.3d 239) court recognized a sliding scale of interactivity under which active websites, those which evidently do trade within the forum state via cyberspace, are subject to personal jurisdiction while passive sites, those that do little more than make information accessible to forum state users, are not. In addition, a rote application of *Zippo*‘s active/passive categorization system can produce invalid consequences depending on the manner in which a site is using geolocation technologies. Where intentional torts are concerned jurisdiction is suitable in the lack of purposeful availment providing the defendant explicitly aimed its tortuous actions towards the forum state. On the other hand, the reasonableness prong concentrates on whether an exercise of jurisdiction would be divergent to established concepts of fair play and substantial justice, an idea that covers the weight on the defendant, the forum state‘s interest in adjudicating the dispute, the plaintiff‘s interest in securing a suitable forum, and generally thought of interstate judicial economy and effectiveness (*Calder v. Jones*, 465 U.S. 783, *International Shoe Co. v. Washington*, 326 U.S. 310; Lanin, 2000, 1448).

In an epoch when actors damage others without either party knowing where the other is located, tying a court’s power to adjudicate the dispute to whether an actor had

intentionally directed his harmful conduct toward a specific geographic place is appealing. As a result, there is a need for an "express aiming at the forum state" (*Pavlovich v. Superior Court*, 58 P.3d 2; Berman 2002). A state court can assert long-arm jurisdiction over a party to a dispute only if that party has "certain minimum contacts with [the forum] such that the maintenance of the suit does not offend 'traditional notions of fair play and substantial justice'" (*Shoe Co. v. Washington*, 326 U.S. 310; Zekos, 2007b). The contacts must show that the party has "purposefully avail[ed] itself of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws" (*Burger King Corp. v. Rudzewicz*, 471 U.S. 462). For instance, the mere likelihood of consulting a website from any actual territorial jurisdiction was considered enough to give rise to a finding of business activity there. No specific attempt to beseech business from citizens of Connecticut (as opposed to those in the other 49 states) was essential to ground competence. Since the defendant had set up a webpage and a toll-free number which could be used by anyone in the U.S., including internet users in Connecticut, instruction must have reasonably foreseen that it could be sued in the state's courts on the basis of its acts (*Inset System v. instruction Set, Inc* 1996 US Dist, LEXIS 7160, *Cybersell Inc. v. Cybersell Inc* U.S. Ct. of Appeals, 9th Circ. (1997)**).**

The question is if whether a bad end product within a geographic location is itself adequate to satisfy the "minimum contacts" test (*Calder v. Jones* 465 U.S. 783, Keeton v. Hustler Magazine, Inc., 465 U.S. 770, *James R. Pielemeier* 2009). For instance, courts are beginning to converge on a set of standards to balance the right to speak anonymously with the rights of those injured by defamatory anonymous speech (*Mobilisa, Inc. v. Doe* 1, 170 P.3d 712; Gleicher, 2008, 349). Moreover, the court in *Independent Newspapers Inc. v. Brodie* held that in a defamation action involving anonymous speakers, a trial court should not order disclosure until five criteria are satisfied (*Indep. Newspapers, Inc. v. Brodie*, 966 A.2d 432; Zekos, 2006). Furthermore, the Doe cases illustrate the evolutionary process by which judges have come to understand how different Internet fora and predominantly message boards, work and what types of conversations take place there(*Doe I v. Individuals*, (*Autoadmit*) 561 F. Supp. 2d 249; Lidsky, 2009). U.S. Supreme Court has to make available definitive guidance as to the appropriate balance between anonymous speech and the protection for reputation. Moreover, the U.S. Supreme Court should embrace a unified approach to personal jurisdiction analysis which turns principally on whether the defendant objectively should be held to be on warning that his conduct was considerably definite to have the influence claimed by the plaintiff to be wrongful in the forum state.

A doctrine of personal jurisdiction seeking to confine extraterritorial behaviour aimed at causing harm inside the forum's borders is attractive. The territory doctrine demands some action that connects the person with the geographic territory of the state. Activities include the person's physical presence within the state's borders (*Pennoyer v Neff*. 95 U.S. 714), past action of the person within the state that generates a claim before a court (*Shoe Co. v. Washington*, 326 U.S. 310), and some status or past action that integrates the individual into the state's political community (*Milliken v. Meyer*, 311 U.S. 457). Activity beyond the state's territorial borders that causes harmful effects within the borders of the state is the late development in personal jurisdiction doctrine constituting sufficient contact with the forum (*Calder v. Jones*, 465 U.S. 783). The behaviour producing the harm has to be "expressly aimed"

at the forum (*IMO Industries, Inc. v. Kiekert AG*, 155 F.3d 254; Stein, 2004, 411). The call for matching prescriptive jurisdiction rules seems the most acute in cyberspace cases. Therefore, harmonization of jurisdiction rules related to cyberspace transactions could lead to more expected outcomes across the globe.

The *Zippo* test has been criticized as too one-dimensional for regular use (*Oldfield v. Pueblo De Bahia Lora, S.A.*, 558 F.3d 1210; *Richard K. Greenstein 2007)*. Established statutory and constitutional principles continue to be the touchstone of the personal jurisdiction inquiry examining a party‘s physical and economic contacts with a state, as well as limitations rooted in the forum state‘s long-arm statute, serving as the focal point (*Best Van Lines, Inc. v. Walker*, 490 F.3d 239). Most cases connecting harms inflicted via cyberspace will rarely implicate purposeful availment making it effortless to cause harm on out-of-state residents without positively relating oneself with the forum state for the rationale of acquiring benefits and rights from that state. As a result, to call for purposeful availment in cyberspace cases is to deny states the capability to guard their interests or those of their citizens (Redish, 1998, 596-600).

Geolocation technologies may perform a role in enabling federalism on cyberspace for years to come (King, 2010). Widespread availability of geolocation tools King) removes the burden from indicating that a jurisdiction was targeted to screening that rational efforts were made to prevent contact with the jurisdiction amounting to an effects test in which an individual is subject to jurisdiction whenever it has targeted a forum and caused harmful effects within the forum via its online acts (Reidenberg, 2005, 1956).

Digitization has noteworthy influence on production and replication, transmission, storage, selective repossession and intelligent processing that give information value in human perspective. Thus, digitization provides a new environment for transmission, retrieval and aggregation of information (*Department of Justice v. Reporters Committee*, 489 U.S. 749). Space in cyberspace is actually a virtual concept derived from, among other things, applications running on your computer and information provided by the server. The content of cyberspace consists only of information. End users (including website owners) deem websites to be business premises. End users’ hope and investment decisions may be best served by treating space in cyberspace like space in real world, and it may also be appropriate to community notions of what constitutes unlawful conduct. Websites are not the result of servers and computer systems alone, but rather they need another fundamental input: information. There are competing interests in controlling entrée to information resources. Legal principles have developed to tackle interests in real world as a separate, independent discipline and so it may be essential to adopt an interdisciplinary approach to reconcile intersecting areas of the law (Frischmann and Moylan, 2000, 875). Thus, cyber-law is about advancement, technological advancement, legal advancement, and the growing relationship between law and technology implicating novel facts and contexts because of fast evolving technologies (Froomkin, 1995, 718; Lidsky, 2000, 885). It could be argued that old legal doctrines can be applied metaphorically to new situations where it is possible.

Internet and globalization produce true conceptual challenges to sovereignty and territoriality. To that extent Goldsmith argues (Goldsmith, 1998) that “territorial regulation of the Internet is no less feasible and no less legitimate than territorial

regulation of non-Internet transactions." The court gets its power to adjudicate a matter from the state and so the perception of Jurisdiction is based on the concept of state. Is there a cyber-state (cyber-country)? Taking into account the current technology and the human nature, a cyber-state cannot come to light.

The real world state lies upon the foundation of sovereignty. The territorial jurisdiction of states and the jurisdictional limits of the municipal courts are based on the territorial theory. State has jurisdiction over all things situated within and over every individual present within its territory (Oxman, 1997, 55). The notion of jurisdiction is based on the perception of sovereignty of the state over its people as well as over its territory. As discussed earlier the absence of conventional geographical borders in cyberspace makes questionable the use of territory as a justification for sovereign jurisdiction. On the other hand, as mentioned above, in cyberspace cases courts have found the connecting elements-interpreting mostly the old legal principles broadly to govern electronic transactions- that allow states to claim state sovereignty which means that in fact states have already claimed their electronic/cyber/virtual state sovereignty.

Moreover, in a globalized world, economic operators no longer work within one national system and their commercial doings extent across regions, countries, and continents. Free accessibility of information collides with the right of the receiving state to guard itself against outside interference, consequently creating regulatory conflicts (*Bangoura v. Washington Post*, 2005 CarswellOnt 4343). Sovereign states attempt to regulate cyberspace causing problems in its use. The Internet's decentralized operation makes it impossible for any single state to control activity in cyberspace. An unregulated cyberspace could lead to the excessive concentration of power in private hands because the lack of regulation means no control on the use of technology by the powerful for private advantage (Cohen, 1998; Schwartz, 1999). Cyberspace cases epitomize the growing category of international conflicts with a public dimension (Buxbaum, 2002, 935-936; Sassen, 2000, 116).

The commercial environment is now global, but legal sovereignties are still territorial. The Internet collapses our traditional notions of location and the significance of geography for sovereignty and regimes of law. The jurisdiction of national courts is based upon the domestic laws of individual countries and the legislative jurisdiction of a State is limited to its territory. Border controls on the Internet are not impossible to develop and implement (*United States v Montoya de Hernandez* 473 US 531) . Many governments already regulate cyberspace. China has suppressed dissidents online and has made it problematical for users to access content available in the United States (Goldsmith and Wu, 2006). Thus, countries, corporations, organizations, and private individuals already regulate the Internet. The U.S. government retains control over the content of the authoritative root zone file (Macavinta, 1999). It is difficult for governments to impose technological limit on what is accessible via the Internet but China controls access to the Internet through centrally regulated servers (Lewis, 1996; Pomfret, 1999). Law is a key part of society's replication and a coercive force. As result the United States has relied on the preservation of state sovereignty as a rationale for regulating exports of encryption technology and for promoting national regulation of Internet gambling. Regulation of Internet activities that originate in another state is an illegitimate encroachment on that state's sovereignty (*American Libraries Ass'n v. Pataki*, 969 F. Supp. 160). To that extent

Noel Cox says that “It is no longer possible for the nation-State to be the sole, or even prime, regulator of economic norms. Decisions respecting the forms of law will be made not at the national level, but internationally” (Noel Cox, nd, 10).

Moreover, a state has come across the new phenomenon of cyber-terrorism and so the control of cyber-terrorism from a technological perspective. As sensitive information is accessible via cyberspace, it is possible the cyber-terrorists to get access to the information and use it to the detriment of the entire global economy. Regardless of the use of modern geolocation technologies, the identity and location of cyber-terrorists are impractical to pin point because they intentionally conceal their location by looping several computer systems in various countries before attacking their objective target. Taking into account the fact that cyberspace is nowhere and everywhere, the attack for purposes of establishing jurisdiction is nearly impossible. Cyber-terrorists can use an anonymous or masked IP address confounding any effort to establish with any accuracy the true location or identity of the attacker. Even more problematic is an attack against a medium itself.

Under the universality principle, each and every state has jurisdiction to try specific offences. Under the principle of universality, any State is authorized to bring to trial people accused of international crimes, in spite of the place of commission of the crime, or the nationality of the doer or of the victim. The foundation behind this special authorization to States to depart from the classic principles of territoriality or nationality was the requirement to mutually fight against a form of criminality that affected all States and so universal jurisdiction was based on a shared alarm of all the States (Bantekas and Nash, 2007, 88). A vital subject will be the determination of presence on national territory, which many states stipulate as a requirement for universal jurisdiction. The universal jurisdiction principle, with the resource of which the state has the title to adopt laws allowing the penalization of certain categories of acts that are considered by the international community as persecuted in its interest.

The territoriality principle lies at the very centre of any legislative endeavor of the state within its territory. As a result the implementation of jurisdictional competences is above all a territorial happening (*ratione loci*). State competences come to life in a specific space and continue bound exclusively thereto. The scope of superiority exercised at an actual territory, shaped by the organs of state power, is complete and exclusive. The state is competent to embark on jurisdictional activities with regard to events happening abroad, but resulting within the state territory. Moreover, international law permits particular liberty of the states on the issue of jurisdictional order. International law rules out an act by one State in the territory of another State which only State officials contrasting to private ones may execute (Akehurst, 1972-73, 145). Violations of this principle counting violations conducted distantly using cyberspace have led to objections by States involved (Lemos, 2002; Goldsmith, 2001). The question to be answered is if there is a need for an alteration of the idea of statehood. Such a necessity results from the fact of the territorial nature of states (Rosenne, 2003) and in the very opposition to “territorially” regulated state relations, the cyberspace is defined as cyber-territorial and not territorial in the sense of the territorial nature of states. Consequently, concerning the limitlessness of cyberspace, its cyber-territoriality (“a-territoriality”) and its common presence, statehood in its conventional substance, or, its territorially described perspective of regulating social and international relations needs to be verified or adjusted with regard to the new

cyber-territorial electronic dominium.

Can the principle of territoriality be applied to cyberspace if it is considered as state's cyber territory? According to Joanna Kulesza it is rather apparent, that the principle of territoriality may not be applied to action taken in cyberspace (Kulesza). The principle of territoriality as defined by the conventional sense; it is rather apparent, that this principle may not be directly applied to action taken in cyberspace but the principle of territoriality modified as the principle of cyber-territoriality is applicable if cyberspace is considered as state's cyber territory. States have begun declaring their jurisdiction outside their own territory with reference to conduct on cyberspace, to the point where this has turned out to be the rule rather than the exception (Ryngaert, 2008, 187; Svantesson, 2007, 1).

The legal right of countries to control the Internet is undoubted and the most effective means to achieve this is to regulate the architecture of cyberspace (Zekos, 1999; *US v Smith*, 680 F 2d 255). The efficacy of the concept of "closest and most real connection" is reduced, in that no part of the world is any more directly affected than any other by events on the web, as information is available simultaneously to anyone with a connection to the Internet (*McConnell Dowell Constructors Ltd v Lloyd's Syndicate* 396 [1988] 2 NZLR 257 (CA)). Law, understood as centralized juridical state power, has lost its importance in modernity and had been eclipsed by power that is specific, local, fragmentary, and dispersed but always the state controls the contribution of power still keeping the centralized juridical state power in tact where it considers necessary to sustain the state power. Government regulates by changing the architecture of the space itself, which means that governments might well be able to control online behaviour even more successfully than they control behaviour in the "real world."

Taking into account that the issue of jurisdiction is entangled with precisely the fixed conception of territorial boundaries, territorially-based sovereigns are facing challenges regulating in an electronic/cyber/virtual environment Aleinikoff, 2000). Cyberspace has expanded sovereignty including an electronic dimension and so this author considers that present regulations of electronic transactions show that states regard cyberspace sovereignty as part of their own sovereignty since electronic actions affect their own territory.

Conclusions

Cyberspace is a global meta-network that allows as an open platform the transmission of information among end users that link computers to the network. Thus, cyberspace in terms of the applications affects end users (Kerr, 2003; Lemley, 2003). There is a need to distinguish between real, including the materials and apparatus, and virtual understandings of cyberspace when we apply law to it (Hunter, 2003, 447-448; Rusch, 2000, 592; Yen, 2002, 1230-31).

The market has a task in generating the borders of multidimensional territories in cyberspace. The extent of privacy in cyberspace principally depends on a solid technical infrastructure. Cyberspace challenges the law's traditional dependence on territorial borders; it is an endless electronic/digital space and place bounded by screens and passwords rather than physical markers. Moreover, cyberspace is

transformed and considered to be just like a place and the development of property interests over cyberspace means that this place is enclosed, and privately exploited. Furthermore, cyberspace as a cyber space and place as it is defined above is a discrete space. The property of sovereignty in physical space has been territorial and cyberspace as electronic space and place is un-territorial. The EU recognized that cyberspace performance can and even has to be regulated in order to find an equilibrium between freedom and control (*EU Information Society Guide* 1996, *eDirectives* 2002).

Cyberspace does not challenge the territorial notion of the state as a collective organization that resides within specific geographical borders but merely the electronic state sovereign based on state cyberspace territory brings a new dimension into the utility of territory and state sovereignty. The exclusivity of sovereign authority, to the exclusion of external forces, is rooted in the relationship between physical proximity and the effects of any particular behaviour which with the emergence of the electronic state sovereign expands its applicability into electronic transactions that finally get again a physical proximity with territorial effects. A nation's prerogative to control events within its territory entails the authority to regulate the national effects of extraterritorial acts including the harmful local effects of electronic activity. Thus, cyberspace activities originating outside the territory but having an effect upon people within the territory of a state are potentially subject to the claims of the sovereign. It should be taken into consideration that the territorial jurisdiction of states and the jurisdictional limits of the municipal courts are still based on the territorial theory.

When the law is expected to solve a problem produced by new technology, it is difficult for the law to "get it right" unless decision makers understand not just the technology, but the social and commercial utilization of the technology as well. It might be necessary to have some international rules for the new international area of cyberspace, just as there are special international rules for international airspace and sea areas. The state parties of Outer Space Treaty did agree that space would be the "province of all mankind," creating an extra-jurisdictional international territory and since the concept of jurisdiction finds its genesis in the concept of territory, the principle of sovereign equality, and noninterference with the national affairs of states, nations will have to employ new and innovative legal regimes in order to exercise legal controls over people in space(Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, Jan. 27, 1967, 610 U.N.T.S. 205). It has to be taken into account that cyberspace, altogether, is an international cyber-"territory." Moreover, The International Law Commission of the United Nations refers to the concept of 'extraterritorial jurisdiction', defining it as 'an attempt to regulate by means of national legislation, adjudication or enforcement the conduct of persons, property or acts beyond its borders which affect the interests of the State in the absence of such regulation under international law'(International Law Commission (ILC), 'Report on the Work of its Fifty-Eighth Session' (1 May-9 June and 3 July-11 August 2006) UN Doc A/61/10). Hague Conference on Private International Law talks about exorbitant jurisdiction as: '[J]urisdiction is exorbitant when the court seised does not possess a sufficient connection with the parties to the case, the circumstances of the case, the cause or subject of the action, or fails to take account of the principle of the proper administration of justice'(Hague Conference on Private International Law,

International Jurisdiction and Foreign Judgments in Civil and Commercial Matters, October 1997). Furthermore, without international rules on enforcement regarding material and electronic transactions, a court's decision over a non-resident will be without effect (*Fair Hous. Council v. Roommates.com*, 521 F.3d 115; *Arista Records LLC v. Does* 1–16, No. 1:08-CV-765, 2009 WL 414060).

The notions, doctrines and laws related to state sovereignty should be directly applicable to the electronic state sovereignty as well. Universal jurisdiction is the most operative method to discourage and avert international crimes by increasing the probability for prosecution and punishment of its perpetrators. The establishment of universal cyber- jurisdiction for cyberspace as an electronic space and place allowing all courts around the globe to deal with the cyberspace transactions and disputes or cyber-crimes such as cyber-terrorism will bring harmony and certainty in electronic trading taking into account that the electronic transactions have the potential to affect simultaneously all jurisdictions. Differences felt by people in real world solved by people in real world and not by a cyber-society means that disputes will be settled by state jurisdiction. It seems that presently there is a variety of factors taking into consideration in order to justify jurisdiction for electronic transactions creating uncertainty. Universal cyber-jurisdiction will mean that any state whose people are affected in any way by an electronic action will have jurisdiction to decide and the decision will be enforced by an international convention of enforcement of foreign courts decisions. The universal cyber- jurisdiction will be especially useful for criminal and intellectual property cases (Zekos, 2007a, 233). The establishment of state cyber-courts having universal cyber jurisdiction dealing with acts taken place within state's cyber territory will bring efficiency in the globalized economy and world.

Electronic state sovereignty and territory can be infinite in an electronic dimension covering any possible electronic space anywhere the electronic signals transferring information travel before received by electronic equipments located within the territory of a state on earth. A state that possesses the most advanced and original technology can intervene and control the cyber-territory of any state as long as there is no possibility to block electronically the intervention in the cyberspace of any state. Therefore, the problem according to this author lies in the fact that the state with supreme electronic technology will establish a more advanced electronic/cyber/virtual state sovereignty rather other less advanced states. In fact electronically independent states will impose the new decision making order to other states less electronically independent. The nature and depth of the electronic state sovereignty of being an endless electronic space depending on the electronic capacity and capabilities of a state accessible from the state sovereignty by the use of electronic technology and not only cyberspace under its current conception might cause frequent conflicts among states because of the overlapping and the fact that electronic actions concurrently affect a number of jurisdictions and so there is a need for an international clarification of some international law principles of non-intervention in order to be applicable in an electronic environment the state's cyber-territory and so state's electronic/cyber/virtual sovereignty. Thus, cyber state sovereignty should be the term for the entirety of international rights and duties that should be recognized by international law regarding this new dimension of the state's sovereignty. Taking into consideration the depth of the use of electronic technology in the states' affairs and their citizens' lives, electronic intrusion of the cyber state sovereignty by the use of

electronic technology will make the state sovereignty an empty letter because everything will be controlled and influenced by the used technology from a distance. Then in the future it cannot be rejected in advance conquer of a state by distance via electronic technology making the defence of state sovereignty an empty letter and vital the defence of the electronic state sovereignty. Cyber state sovereignty and state sovereignty coincide considering having the same borders for the placement of the current electronic apparatus used to have access of the electronic state sovereignty but not only are different concepts but also the depth of cyber state sovereignty is changeable without borders depending not only on the capacity of the used electronic technology in order to have access but also on the nature of the electronic networking which comprises the electronic/cyber state sovereignty.

Bibliography

Philip E. Agre, (1998) 'Yesterday’s Tomorrow', Times Literary Supplement July 3, 1998.

Michael Akehurst, (1972-73) 'Jurisdiction in International Law' 46 British Yearbook of International Law 145.

Alexander Aleinikoff, (2000) 'Sovereignty Studies in Constitutional Law: A Comment', 17 Const. Comm. 197.

Shulamit Almog, (2002) 'From Sterne and Borges to Lost Storytellers: Cyberspace, Narrative, and Law', 13 Fordham Intell. Prop. Media & Ent. L.J. 1.

Natasha Bajema and Mary Beth Nikitin, (2004) 'Assessing Nuclear Maturity: Determining Which States Should Have Access to What Nuclear Technology', 28 Fletcher F. World Aff. 157.

Illias Bantekas and Susan Nash, International Criminal Law (Routledge 2007).

Catherine M. Barrett, (2002) 'FBI Internet Surveillance: The Need for a Natural Rights Application of the Fourth Amendment to Insure Internet Privacy', 8 Rich. J L. & Tech. 16.

Yochai Benkler, (2000) 'From Consumers to Users: Shifting the Deeper Structures of Regulation Toward Sustainable Commons and User Access', 52 Fed Comm. L.J. 561.

Paul Schiff Berman, (2002) 'The Globalization of Jurisdiction', 151 U. Pa. L. Rev. 311.

James Boyle, (1997) 'Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors', 66 U. Cin. L. Rev. 177.

Caroline Bradley & A. Michael Froomkin, (2004) 'Virtual Worlds, Real Rules', 49 N.Y.L. Sch. L. Rev. 103.

Ian Brownlie, Principles of International Law (Oxford University Press 1999).

Dan L. Burk, (2000-2002) 'Legal Consequences of the Cyberspatial Metaphor', in 1 Internet Research Annual: Selected Papers from the Association of Internet Researchers Conferences 2000–2002.

Hannah L. Buxbaum, (2002) 'Conflict of Economic Laws: From Sovereignty to Substance', 42 Va. J. Iint'l L. 931, 935-936

Eric Cafritz and Omer Tene, (2002-2003) 'Article 113-7 of the French Penal Code: The Passive Personality Principle' 41 Columbia Journal of Transnational Law 585.

Edward Castronova, (2004) 'The Right to Play', 49 N.Y.L. Sch. L. Rev. 185.

Julie E. Cohen, (1998) 'Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management', 97 Mich. L. Rev. 462.

Julie E. Cohen, (2000) 'Examined Lives: Informational Privacy and the Subject as Object', 52 Stan L. Rev. 1373.

R.A. Conrad, (2001) 'Searching for Privacy in All the Wrong Places: Using Government Computers To Surf Online, 48 Naval L. Rev. 1, 38.

Noel Cox, 'The regulation of cyberspace and the loss of national sovereignty' p10. < www.ssrn.com>.

Convention on Cybercrime, Nov. 23, 2001, Europ. T.S. No. 185, available at <http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm>.

James Crawford, The Creation of States in International Law (Clarendon Press 1979).

eDirectives: Guide to European Union Law on ECommerce- Commentary on the Directives on Distance Selling, Electronic Signatures, Electronic Commerce, Copyright in the Information Society, and Data Protection, (Kluwer Law International 2002).

Nina Elkin-Koren, (2001) 'Let the Crawlers Crawl: On Virtual Gatekeepers and the Right to Exclude Indexing', 49 J. Copyright Soc'y U.S.A. 165.

Niva Elkin-Koren and Eli M. Salzberger, (1999) 'Law and Economics in Cyberspace', 19 Int'l Rev. of L. & Econ. 553

Amitai Etzioni, (2002) 'Implications of Select New Technologies for Individual Rights and Public Safety' 15 Harv. J. of L. & Tech. 257.

Bardo Fassbender, (1998) 'The United Nations Charter as Constitution of the International Community', 36 Colum. J. Transnat'l L. 529.

Todd H. Flaming, (1997) 'The Rules of Cyberspace: Informal Law in a New Jurisdiction', 85 Ill. B.J. 174.

Richard Freer, 'American and European approaches to personal jurisdiction based upon internet activity', Public Law & Legal Theory Research Paper Series Research Paper No. 07-15, Emory University School of Law.

Brett Frischmann & Dan Moylan, (2000) 'The Evolving Common Law Doctrine of Copyright Misuse: A Unified Theory and Its Application to Software', 15 Berkeley Tech. L.J. 865.

Michael Froomkin, (1995) 'The Metaphor is the Key: Cryptography, the Clipper Chip, and the Constitution', 143 U. Pa. L. Rev. 709.

Bill Gates, Business @ The Speed of Thought: Using a Digital Nervous System (Grand Central Books 1999).

Owen Gibson, (2003) 'Internet café guilty of piracy', Media Guardian Jan. 28, 2003.

Bernard Gilson, The Conceptual System of Sovereign Equality. (Leuven: Peeters 1984).

Nathaniel Gleicher, (2008) Note, 'John Doe Subpoenas: Toward a Consistent Legal Standard', 118 Yale L.J. 320.

Jack Goldsmith, (1998a) 'Against Cyberanarchy', 65 U. Chi. L. Rev. 1199.

Jack L. Goldsmith, (1998b) 'The Internet and the Abiding Significance of Territorial Sovereignty', 5 Ind. J. Global Legal Stud. 475 (1998)

Jack Goldsmith (2001) 'The Internet and the Legitimacy of Remote Cross-Border Searches' University of Chicago Legal Forum 103.

Jack Goldsmith and Tim Wu, Who Controls the Internet? Illusions of a Borderless World (Oxford University Press 2006).

Ryan Goodman and Derek Jinks, 'Toward an Institutional Theory of Sovereignty', Harvard Law School Public Law Research Paper No. 57.

Richard K. Greenstein, (2007) ' The action bias in American law: internet jurisdiction and the triumph of Zippo dot com', Temple Law Review 21.

Mika Hayashi 'The Information Revolution and the Rules of Jurisdiction in Public International Law' in Myriam Dunn, Sai Felicia Krishna-Hensel, and Victor Mauer (eds), The Resurgence of the State (2007: Ashgate).

Alan Hunt (1992) 'Foucault’s Expulsion of Law: Toward a Retrieval', 17 L. & Soc. Inq. 1.

Dan Hunter, 'Cyberspace as Place and the Tragedy of the Digital Anticommons', 91 Cal. L. Rev. 439.

David R. Johnson, Susan P. Crawford & John G. Palfrey, Jr. (2004) 'The Accountable Internet: Peer Production of Internet Governance', 9 Va. J.L. & Tech. 9.

A Johnson-Laird The Internet: the good, the bad and the ugly' The Computer Law Association
Computer Law Companion Vol III 81, 100 (C. Ian Kyer & Christopher E. Erikson eds., 1996)

Hans Kelsen General Theory of Law and State (Russell and Russell 1961).

Orin S. Kerr (2003) 'The Problem of Perspective in Internet Law', 91 Geo. L.J. 357.

Kevin F. King, 'Personal Jurisdiction, Internet Commerce, and Privacy: The Pervasive Legal Consequences of Modern Geolocation Technologies'. <www.ssrn.co>.

Kevin F. King (2010) 'Geolocation and federalism on the internet: cutting internet gambling's Gordian knot', 11 Columbia Science and Technology Law Review 41 www.stlr.org.

S Krasner, S. (1988) 'Sovereignty: an institutional perspective', 21 Comparative Political Studies 66.

Joanna Kulesza, 'Internet governance and the jurisdiction of states: justification of the need for an international regulation of cyberspace', (December 02, 2008). III GigaNet Symposium Working Paper. Available at SSRN: http://ssrn.com/abstract=1445452

Ari Lanin, (2000) 'Who Controls the Internet States' Rights and the Reawakening of the Dormant Commerce Clause', 73 S. Cal. L. Rev. 1423.

F. Gregory Lastowka & Dan Hunter (2004) 'The Laws of the Virtual Worlds', 92 Cal. L. Rev. 1.

Mark A. Lemley (2003) 'Place and Cyberspace', 91 Cal. L. Rev. 521.

Robert Lemos (2002) 'Russia accuses FBI agent of hacking', cnet news, 16 August 2002

Lawrence Lessig (1996) 'Reading the Constitution in Cyberspace', 45 Emory L.J. 869.

Peter H. Lewis, (1996) 'Limiting a Medium Without Boundaries', N.Y. Times, Jan. 15, 1996, at D1.

Peter L. Lindseth, Power and legitimacy: reconciling Europe and the nation-state (Oxford University Press 2010).

Jessica Litman (1999) 'Breakfast with Batman: The Public Interest in the Advertising Age', 108 Yale L.J. 1717.

Lyrissa Barnett Lidsky (2000) 'Silencing John Doe: Defamation & Discourse in Cyberspace', 49 Duke L.J. 855.

Courtney Macavinta (1999) 'ICANN to Control Domain Name Server', cnet news, June 30, 1999.

Fabrizio Marrella and Christopher S. Yoo, Is Open Source Software the New Lex Mercatoria? U of Penn, Inst for Law & Econ Research Paper No. 07-19; U of Penn Law School, Public Law Research Paper No. 07-31; (2007) 47 Virginia Journal of International Law 807 Available at SSRN: http://ssrn.com/abstract=1007236

N Masilamani and John Anup Kurvilla (2001) 'The Future of State Sovereignty: Emerging Concerns in the Internet Era', 13 The Student Advocate.

David McGowan (1998) Website Access: The Case for Consent, 35 Loy. U. Chi. L.J. 341.

Ralf Michaels (2004) 'Territorial jurisdiction after territoriality' in Piet Jan Slot and Mielle Bulterman (eds.), Globalisation and Jurisdiction Kluwer Law International 105.

Neil Weinstock Netanel (2000) Cyberspace Self – Governance: A Skeptical View from Liberal Democratic Theory 88 Calif. L.Rev. 395.

Bernard Oxman 1997) 'Jurisdiction of States' in: Encyclopedia of Public International Law vol 3 (Elsevier 1997) 55.

James R. Pielemeier (2009) 'Why General Personal Jurisdiction Over "Virtual Stores" is a Bad Idea' 27 Qinnipiac Law Review 625.

John Pomfret, (1999) 'Chinese Sentenced in Internet Case', Wash. Post, Jan. 21, 1999, at A19

David G. Post (1998) 'The "Unsettled Paradox": The Internet, the State, and the Consent of the Governed', 5 Iind. J. Global Legal Stud. 521.

Martin Redish (1998) 'Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution', 38 Jurimetrics J. 575.

Joel Reidenberg (1996) 'Governing Networks and Rule-Making in Cyberspace', 45 Emory L.J. 911.

Joel Reidenberg (2005) Symposium: 'Current Debates in the Conflict of Laws: Choice of Law and Jurisdiction on the Internet: Technology and Internet Jurisdiction', 153 U. Pa. L. Rev. 1951.

Arno R. Rodder and Henrik W.K. Kaspersen (eds.) (1996) EU Information Society Guide, The EU Committee of the American Chamber of Commerce in Belgium, (Brussels 1996).

Michel Rosenfeld (2008) Rethinking Constitutional Ordering in an Era of Legal and Ideological Pluralism, 6 Int'l J. of Const. L. (I.CON) 415.

S. Rosenne (2003) The perplexities of modern international law, General Course on Public International Law, RCADI tom III.

Jonathan J. Rusch (2000) 'Cyberspace and the "Devil's Hatband"', 24 Seattle U. L. Rev. 577.

Cedric Ryngaert Jurisdiction in International Law (Oxford University Press 2008) 187.

Saskia Sassen (2000) 'The State and Economic Globalization: Any Implications for International Law?' 1 Chi. J. Int'l L. 109.

Thomas Schultz (2008) 'Carving up the Internet: Jurisdiction, Legal orders, and the Private/Public International Law Interface' 19 European Journal of International Law 799.

Paul M. Schwartz (1999) 'Privacy and Democracy in Cyberspace', 52 Vand. L. Rev. 1607.

Hideaki Shinoda, Re-Examining Sovereignty: From Classical Theory to the Global Age (Macmillan 2000).

Edward Soja (1996) 'Surveying Law and Borders: Afterword', 48 Stan. L. Rev. 1421.

Allen R. Stein, (2004) 'Symposium, Personal Jurisdiction and the Internet: Seeing Due Process Through the Lens of Regulatory Precision', 98 NW. U. L. Rev. 411.

Cass Sunstein, Designing Democracy: What Constitutions Do, (Oxford University Press 2001).

Dan Jerker B. Svantesson Private International Law and the Internet (Kluwer Law International 2007).

Damian Tambini, Danilo Leonardi and Chris Marsden Codifying Cyberspace: Communications self-regulation in the age of Internet convergence, (Routledge 2008) .

The Electronic Signatures in Global and National Commerce Act ("E-Sign"), 15 U.S.C. §§7001-7031 (2000).

The Uniform Electronics Transaction Act, ("UETA"), 7A U.L.A.§701

Alexander Wendt (1992) 'Anarchy Is What States Make of It', 46 Int'l Org. 391.

Stephan Wilske & Teresa Schiller (1997) 'International Jurisdiction in Cyberspace: Which States May Regulate the Internet?', 50 Fed. Comm. L.J. 117.

Theodore D. Woolsey Introduction to the Study of International Law (5th ed New York, Charles Scribner's Sons 1883).

Timothy S. Wu, Note (1997) 'Cyberspace Sovereignty? — The Internet and the International System', 10 Harv. J.L. & Tech. 647.

Jeffrey Yeates, (2001) 'CALEA and the RIPA: The U.S. and the U.K. Responses to Wiretapping in an Increasingly Wireless World', 12 Alb. L.J. Sci. & Tech. 125, 131-134 (2001).

Alfred C. Yen (2002) 'Western Frontier or Feudal Society?: Metaphors and Perceptions of Cyberspace', 17 Berkeley Tech. L.J. 1207.

G Zekos (2003) 'Trademarks as Domain Names: Techno-Legal Aspects of Information Society and New Economy', Formatex, Spain www.formatex.org.

G Zekos (2005) 'Cyberspace Sovereignty and Jurisdiction', 1 The ICFAI Journal of Cyber Law www.icfaipress.org.

G Zekos (2006) 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction in Cyber Crimes and Cyber Torts', May 2006 ICFAI Journal of Cyber Law 9 www.icfaipress.org.

G Zekos (2007a) Cyberspace Sovereignty and Jurisdiction, in C Vidya (ed) Cyber Jurisdiction: A Legal Vision,(The ICFAI University Press 2007) www.icfaipress.org/books.

G Zekos (2007b) Economics, Finance and Law on MNEs Nova Publishers, New York www.novapublishers.com.

G. Zekos (2007c) 'State Cyberspace Jurisdiction and Personal Cyberspace Jurisdiction' 15 Int J Law Info Tech 1; doi: 10.1093/ijlit/eai029.

G Zekos (2008a) Economics and Law on Competition in US and EU (Nova Science Publications New York USA 2008). www.novapublishers.com.

G Zekos (2008b) Intellectual Property Rights and Cyberspace (Amicus Books, The ICFAI University Press 2008), www.iupindia.gr .

G Zekos (2008c) Issues of Cyberspace and E-commerce, 2008 (Amicus Books, The ICFAI University Press 2008), www.iupindia.gr.

Jonathan Zittrain (2003) 'Internet Points of Control', 44 B.C. L. REV 653 (2003).