Management Studies, Nov.-Dec. 2016, Vol. 4, No. 6, 256-265
doi: 10.17265/2328-2185/2016.06.003

Cyberspace: A New Threat to the Sovereignty of the State

Jackson Adams, Mohamad Albakajai
University of Essex, Colchester, UK

This paper discusses one of the contemporary challenging issues—it is the challenge of e-commerce to the sovereignty of the state, where governments are unable to implement their own laws on disputed cases resulting from trans-border e-commerce interactions. The objective of the current research is to draw attention to the impact of international characteristics of e-commerce on the sovereignty of state, and to identify the factors affecting this sovereignty. The issue of the dynamicity of time and place will be taken into consideration, where activities carried out over the internet are characterized by their cross-border dimension. Based on real e-commerce case studies disputed on international level, this paper will draw on the legal perspective of cyberspace, identifying the relationship between cyberspace and state sovereignty, and outlining the mechanisms by which cyberspace could cross borders and the territory of the state despite all the precautions taken by the state to protect its sovereignty.

Keywords: cyberspace, sovereignty, time, space, soft law

Introduction

The internet has always been recognized as a global decentralized computer network system or a network of networks (Chaffey & Ellis-Chadwick, 2012). Therefore, activities conducted over this network may acquire a cross-border dimension, where people of different countries could be affected by these activities; and hence, different laws, regulations, and policies may apply in cases of legal disputes.

Sovereignty in its traditional concept is based on two key elements: the physical space and territoriality. Thus, sovereignty is defined, in relation to the notion of national boundaries, in three dimensions which are: territory, air, and sea where the state aims to impose national law and national power. Therefore, sovereignty appears as an absolute concept where no authority or external force can compete with the national government in its territories. Bellanger (2011, p. 3) has made a comparison between state sovereignty and cyberspace stating that: “States are places. The Internet is a link. Sovereignties are defined in limited physical space. Internet is a dimension that connects all areas. Although there are many and different States, the Internet is universal one.”

According to the above quote, the internet or the whole cyberspace seems to be no more than a virtual link among the network nodes, and as such it cannot be regarded as a legal entity which is bounded by geographical or physical boundaries that maintain the sovereignty or control of any specific state. Also, the virtual nature of the cyberspace implies dematerialization (everything is paperless), detemporalization (instant communication), and deterritorialization (breaking the geographical boundaries and distances) of online activities and

Jackson Adams, Ph.D., e-commerce, Essex Business School, University of Essex, Colchester, UK.
Mohamad Albakajai, Ph.D., e-commerce, Essex Business School, University of Essex, Colchester, UK.
Correspondence concerning this article should be addressed to Jackson Adams, Essex Business School, Room EBS 323, University of Essex, Wivenhoe Park, Colchester CO4 3SQ, UK.

interactions. The combined effect created by such virtualization process leads to the notion of ubiquity (Schultz, 2004). Hence, the impact of cyberspace on sovereignty can be recognized through the temporal and spatial dimensions.

The current paper will investigate how the cyberspace may impact the sovereignty of the state by disabling some of its own national laws in cases of online disputes, such as those resulting from trans-border e-commerce interactions. The objective will be the highlighting of the impact of e-commerce on the state sovereignty and attributing it to the concepts of temporality and spatiality of the disputed case. The first section will review the political and legal perspectives of previous research on cyberspace and sovereignty. Then, the impact of the time-space theory on the legal perspective of the cyberspace will be explored.

Cyberspace and Sovereignty: Prior Research

Previous research tended to elaborate on the relationship between cyberspace and the state sovereignty emphasising the political, technical, and legal dimensions. For instance, Lewis (2010) has claimed that the early designers and developers of the internet technology had a political desire to satisfy the wishes of the capitalists in USA. The primary wish was limiting governmental powers by making the network widely open, stateless connection to the whole globe without having a central command node (Schneider, 2013). Later on, these characteristics of the internet have played a significant role in downplaying the role of governments in regards to controlling the cyberspace activities and interactions. Therefore, Choucri and Clark (2013) have recognized the political nature attributed to cyberspace activities which have become a major concern to national security of the state, pointing out how “The cyberspace concept has changed from being a matter of low politics to become high politics of national security” (p. 68).

In their argumentation, the two researchers have relied on the recent cases of Wiki leaks and the social media (as in the case of Arab Spring)—which undermined the security and sovereignty of so many states worldwide. However, the media is full of similar news about virtual wars and cyber-attacks which call the attention of both legislators and regulators, for example, McGuffin and Mitchell (2014) have discussed cases, such as the 2007 cyber-attack against Estonia and the 2008 virtual war against Georgia which has a disputed territory with Russia, namely, South Ossetia. In fact, such cases require the international co-operation in combating cyberspace security violations. So, the military tactics and strategies have started to combine the traditional combat with the electronic or virtual attacks (Deibert, Rohozinski, & Crete-Nishihata, 2012). Such cyber activities have made cyberspace acquire a very significant strategic position which could be regarded as equal as geographical spaces, such as land, sea, and air.

Cyberspace has played a role in individualizing the user by allowing him/her to enjoy total liberation from the state or government control, and this could be interpreted as a violation to the sovereignty of the state (Grosso, 2001). An example of this can be seen through carrying out e-commerce transactions, where the individual is free to exercise his/her loyalty to the country that he/she is conducting their business activities in. Doing so indicates that the e-commerce user’s own interests take precedence over that of the state or a social group. It is a practice where the individual seems to oppose external interference with own interests by governmental or societal institutions. This is an attempt of creating own virtual space where the acquired controlling power makes the individual a power block.

As for the legal perspective, Cruquenaire and Lazaro (2013) have tried to expose the problematic nature of the international contracts that are drawn over the Internet. It poses a jurisdictional dilemma (personal or

subject-matter) where no single state can look into disputes arising from such contracts, and where no specific law can be applied without prejudicing the rights of at least one of the disputing parties (Hedley, 2003).

In response to such dilemmas, Jacquot and Weitzel (2001) highlighted the need to adopt new legal systems in order to regulate the cyberspace issues in general and the e-commerce activities in particular. In this regard, traditional laws and legislations have often been criticized for their inability to cope with the fast advances of the cyberspace uses and huge demands for resolving online disputes. In response to this problem, researchers such as: Grewlic (1999), Choucri and Clark (2013), and Kucklich (2009) have called on the international law to allow for the participation of the individuals and businesses in making the cyberspace laws—it should not be limited to the legislative and regulative efforts of the state only. This can be done through involving civil organizations and institutions in every country. Other researchers, such as Sarr (2012) and Jacquot and Weitzel (2001) called for the use of the soft laws, arbitrage, and mediation as means to resolve international disputes of e-commerce, because these means are characterized by their easy and quick procedures and flexibility in contrast with the national or international traditional means.

The law is set to deal with disputable issues as well as with criminal acts that may threaten the security, safety, and stability of the state. Cyberspace seems to be a harbour for criminals whose security-breaching behaviours may undermine the sovereignty of the state in one way or another. Lin (2012) has argued how the cyberspace is infested with cybercrime and cyberterrorism, explaining that: “The modern thief can steal more with a computer than with a gun. Tomorrow’s terrorist may be able to do more damage with a keyboard than with a bomb” (p. 75). The cyber-criminal activities become more complicated because of the boundarylessness of the internet which implies blurring the boundaries between the states.

In general, the literature has mostly focused on debating the inability and harmonization of the international law to deal with cyberspace cases; and how online activities may infringe on the sovereignty of the state. However, the literature did not properly address the roots of this dilemma that may lie in people’s conceptualization of time and space which was the basis for formulating the traditional laws. The new conceptualization is a virtual one that relies on no association to established temporal and spatial boundaries which the researchers used to know before the emergence of cyberspace. Such research gap will be the driving theme of the current study which argues that the temporal and spatial characteristics of the internet must be taken into consideration when formulating the cyberspace laws. This is done by focusing the current investigation on the impact of cyberspace on the sovereignty of the state through three case studies: France v Yahoo in 2006, China v Google Company, and France v Miditext.com in 2000.

Cyberspace: Time-Space Theories & Legal Perspective

The most significant and distinguishing characteristic of the contemporary telecommunication technology is the time-space compression (Hassan, 2003; 2009; Lee & Sawyer, 2010; Thrift, 2006). The problem in cyberspace activities is that they occur outside of the real time and take place from anywhere. According to Wynn and Katz (1997), the cyberspace enabled asynchronous communication, which is distinguished from the synchronous communication which occurs inside the real time-space. In the postmodern world, the physical world has been gradually replaced by the new technology world. Matusitz (2014, p. 717) confirmed that: “The cyberspace put an end to geography. Businesspeople are only a mouse click away from Web users in Vietnam or Guatemala. This also implies the death of the time. So the era of three-dimensional public sphere may become passé.”

On one hand, Laguerre (2004) has attributed the collapse of temporal boundaries and the compression of time distance to cyberspace. On the other hand, Sheldon (2014) argued that cyberspace can still be regarded as similar to other geographical spaces (land, sea, air, and space), explaining that:

> The physical segment of cyberspace—the computers, cables, and satellites, among other physical infrastructure—is geographically situated and operated and maintained by human beings who must, by necessity, live on the land in politically organized communities in physically distinct and demarcated territories. (p. 268)

It is worth noting here that the cyber power is less visible than other forms of power, since it is totally reliant on "information"—which is quite invisible or intangible. Thus, in interpreting the nature of space, Mihalache (2002) has referred to the concept of time and used the expression of "cyberspace-time continuum" to indicate that the cyberspace is the area where the cyber populations share ideas and information. He pointed out that:

> The only thing that mediates all informational exchanges is time. One buys my information and pays with his time; I buy my information and pay with my time. Time plays in cyberspace the part that money plays in real life; time is money. (p. 300)

Legal theorists have differed in their views about the nature of the cyberspace: some regarded it as no space and attributed it with a sense of fantasy rather than describing it as a real thing; while others have considered it as a true international space. For some, it was geographically separate area—a real space, international, independent, and separated from the territory of the states (Deibert et al., 2012). Yet, the anonymity and autonomy of cyberspace facilitate aggression against state sovereignty and make it quite difficult to identify and locate trespassers (Placid & Wynekoop, 2011). This creates legal challenges as well as problematic jurisdictional vacuums. Also, the intercultural characteristics of cyberspace contribute to the jurisdictional problem and call for cyber-jurisdictions, as explained by Matusitz (2014, p. 713): "Cyberspace is the Global Village, a sphere for interaction between users from multiple cultural backgrounds. It can unite people or divide them for motives rooted in ideology, politics, historical background, race, or religion."

In contrast to the geographically-based view of the cyberspace, an alternative view was proposed by other researchers, who conceive cyberspace as a virtual or a synthetic world (Kucklich, 2009). Thus, in the military view, the cyberspace has been considered as the fifth domain of military operations (land, sea, air, space, and cyber). However, McGuffin and Mitchell (2014) argued that cyberspace possesses the characteristics to be a realm of human interaction but it lacks the characteristics to be considered a domain akin to the domains of land, sea, air, and space; they have also stated that there are military purposes for cyberspace as demonstrated by Russia vs. Estonia, Russia vs. Georgia, and USA vs. Iran. Accordingly, cyberspace is being used for military operations:

> The real environments (land, sea, and air) have become known as "domains" in military terminology, so the domains are where the activity takes place to create effects and ultimately compel an adversary to comply with the will of the victorious state. (McGuffin & Mitchell, 2014, p. 398)

Finally, it is obvious that the ability to communicate in real time globally and to connect people everywhere makes certain laws and legislations of the state violated by the cyberspace. But, these significant characteristics do not make the cyberspace as a material space. It is true that cyberspace can not be considered as a new space in the geographical sense. In contrast, nobody can ignore the argument that cyberspace is a new social space, a "living environment" (Matusitz, 2014), which deserves its own legal analysis. Thus, there should

be a search for new means to regulate the cyberspace, such as soft laws or arbitration (Sarr, 2012; Jacquot & Weitzel, 2001).

The legal challenge associated with cyberspace activities is caused by the fact that cyberspace is a decentralized network, with the ease of accessibility by masses of people and the ability to allow making three types of communication configurations (which no-other media can combine simultaneously): one-to-one, one-to-many, and many-to-many (Biegel, 2001). Again, communications made the internet networks happen independently without considering any territorial account—an independent state of cyberspace (Kucklich, 2009).

For some, the independence of the cyberspace seemed quite threatening and hence they called for governmental interference to control the cyberspace and to protect the state's sovereignty (Lewis, 2010). This is an opposition to the non-governmental approach which emphasizes the role of the individuals in re-organizing the cyberspace. This feeling of unease against the boundarylessness nature of cyberspace has already pushed so many governments to develop and control policies and design procedures or mechanisms that are capable of monitoring their own cyberspace and maintain the sovereignty of their states.

The Tempo-Spatial Element of Cyberspace

Time acceleration is a significant attribute of the cyberspace which makes national laws unable to keep up to date with technological developments (Choucri & Clark, 2013). This creates legal uncertainty in the national legal system leading the concept of sovereignty into an abyss, for example, e-commerce allows the execution and exchange of contracts in an extremely short time with quick and simple click (Laguerre, 2004). Thus, the consumer does not have enough time for a deep consideration about the transaction; certainly, most national laws on distance selling have introduced a right of retraction. However, this right is not really known to most consumers and there are a number of exceptions related to that right, for example it may not be exercised in the context of a sale by auctions (Sarr, 2012). Then the law should find a way to protect the consumers against ill-made decisions or when they fall as a victim to fraud.

Spatiality is another attribute of the cyberspace that poses a great challenge to the concept of territoriality in law. In the traditional sense of territoriality, the state derives its sovereignty from its ability to exercise its domination and control over its territory by imposing its own legislative power. This sovereignty is usually delegated by the individuals to the public authority, and that is why it is described as vertical on the national level. By contrast and on the international level, sovereignty is horizontal where there are sovereign entities beside each other, but each state can not impose its law on other states (Maljean-Dubois, 2003). In case of having absolute sovereignty, the state must have the power to impose its legislations internationally. So, imposing national legislation is not enough to exercise absolute sovereignty.

As for the cyberspace, the power of the state is quite limited, since there is a confrontation between two contradictory concepts: the national sovereignty based on physical and spatial elements on one hand, and a virtual extra-territorial cyberspace on the other hand that transcends the principle of territoriality and robs it off its meaning (Choucri & Clark, 2013). Users of the cyberspace seem to be living in-between two worlds: the traditional physically or geographically bounded world and the virtual transnational world. Thus, legally, the state is not completely removed by the cyberspace which is not a new space outside the state, it is within it. This has been clearly pointed out by Kobrin (1997): "We are not witnessing the end of the state, but rather in front of a reduced effectiveness of the political, economic, and legal authority rooted in the geographical sovereignty" (p. 38).

However, traditional legislation based on territoriality and state sovereignty has remained inadequate and threatened by the cyberspace (Cruquenaire & Lazaro, 2013), for example, the “Yahoo” case in France is a clear example of the impact of cyberspace activities on the sovereignty of the state by violating the French national legislations. The Yahoo site is one of the Internet service providers (ISPs) that provide e-mail service, news, weather, finance, shopping, and auction. The company has a French site in French language.

In 2000, “Yahoo.com” opened a cyber-auction and started selling Nazi memorabilia, although such activity is against the criminal French law which prohibits in the sale or displays anything incites racism (section R645-1 of French Criminal Code). But this kind of selling is legal in the USA law. Anti-racism organizations in France, such as the International League against Racism and Anti-Semitism (LICRA), Union des Etudiants Juifs de France (UEJF), and Mouvement contre le Racisme, l’Antisemitisme et pour la Paix (MRAP) made a claim against Yahoo company. On May 22, 2000, the Tribunal de Grande Assistance de Paris ruled that Yahoo had committed an offense to the collective memory of the country by allowing online auctions of neo-Nazi objects in cyberspace, and the exhibition, in view of its sale of Nazi objects, is contrary to French law (Levy, 2000). Also, “Yahoo! Inc. was ordered to prevent access from French territory to the Nazi objects and hate speech sites in question, or face a penalty of 100,000 francs per day for noncompliance within two months” (Kohl, 2007, pp. 201-202).

In reaction to this court judgment, Heather Killen, a Yahoo! vice president, commented: “It’s very difficult to do business if you have to wake up every day and say ‘OK, whose laws I follow? We have many countries and many laws but just one Internet’” (Cohen-Almagor, 2012, p. 355). On July 24, 2000, when the parties resumed the trial, the Tribunal reaffirmed the order.

However, considering that the selling of Nazi memorabilia is legal in the USA, the company filed a legal suit on its home soil: the Federal District Court for the Northern District of California which considered the important differences between the French legal norms and the American First Amendment and ruled on November 2001 that the French order against Yahoo could not be enforced in the USA. Judge Jeremy Fogel concluded that the French ruling was inconsistent with the First Amendment, and held that, while France could regulate speech in its territory, this (US) court would not enforce a (French) foreign order that violated the protections granted under the US Constitution. Yahoo! showed that the threat to its constitutional rights was real and immediate.

The trial resumed in January 2006 before the US Court of Appeal, (three of eleven judges) concluded that Yahoo!’s claim was not “ripe for adjudication” and should be dismissed on those grounds. Because LICRA and UEJF had not sought enforcement of the French court’s orders in the USA, the French court may not impose a fine even if they do ask for one, and it is unlikely a US court would enforce such a fine even if a French court imposed one. Enforcement is unlikely “not because of the First Amendment, but rather because of the general principle of comity under which American courts do not enforce monetary fines or penalties awarded by foreign courts” (Cohen-Almagor, 2012, p. 357).

The other case study that can be taken as an example of conflicting laws in regards to cyberspace activities is the case of Google. In 2002, Google removed more than 100 controversial sites from Google.fr (France) and Google.de (Germany). Those controversial sites were related to anti-Semitic or pro-Nazi issues. However, those sites were not removed from the main Google.com, which was still accessible from those countries. Those countries were able to impose censorship on Google.com, but this action may also lead to giving up

some of their sovereignties, because this censorship will raise concerns in regards to the democratic legitimacy that is granted in their institutions.

Again, in 2006, Google.cn was launched in China but it was forced by the communist government in China to accept self-censorship (Hartnett, 2011). In accepting such censorship, Google must remove and withhold any information related to democratic, religious, or human rights issues (Brenkert, 2009). However, in 2009, Google was the victim of cyber-attack which was promoted by the Chinese government in an attempt to hack the email accounts of some human rights activists. This has resulted into an international conflict between China and Google, which in 2010 stopped working under the Chinese censorship and redirected its activities to Hong Kong (Tan, 2012). That conflict soon became an international dispute between China and US governments. This proves the idea that no country can enforce its own legal system on other countries.

The above case studies indicated that the cyberspace can easily cross the borders without taking into consideration the sovereignty of the state. Usually, each state imposes its laws on the national level; however, the international use of cyberspace weakens the effectiveness of these laws and the ability to apply them on the international level as indicated by the previous examples. Usually, the rules of private international law still allow courts to assert the priority of national law. However, in the case of cyberspace which transcends all boarders, it becomes almost impossible to apply these laws internationally speaking. So the cyberspace affects two main aspects of the state and its sovereignty; the territory and law that are recognized as the corner stone of the identity of the state, without which sovereignty is lost.

A Vouch for Alternative Legal Mechanisms

The use of alternative means to regulate cyberspace, such as the participation of the private actors led indirectly to weakening the power of the state sovereignty by obliging the states to delegate powers by resorting to independent administration to regulate the cyberspace, for example, e-commerce takes place in a market that transcends all the borders and it is exercised by actors with different legal systems. The rules of national and international law are not enough to regulate relationships that develop on digital networks. However, the specificity of digital networks makes it difficult and probably impossible to regulate the electronic transactions by the government, because the national procedures take long time and are relatively of a fixed nature. Also, on international level, a consensus can’t be easily established to determine the set of rules applicable to cyberspace. Then, the states seek the cooperation with private actors to regulate the e-commerce and adopt a soft law which is a new form of social regulation of cyberspace (Duplessis, 2007). These soft rules are characterized by the simplicity of the process of elaboration, and being practical and flexible. Furthermore, they easily adapt to the complex issues of the Internet, because they rely on the activity of actors who are actually controlling the network (technical players, academics, associations or merchants, consumer associations, and sometimes other actors, such as state actors).

As far as the self-regulating of e-commerce, French state authorities have understood too early the problem of applying the national rules internationally: In 1997, Lionel Joplin, the French prime minister asserted the idea that “it would be unrealistic to expect any public intervention, the state is not intended to replace itself with private actors, information society; individuals, businesses, and local authorities” (Sarr, 2012, p. 56). Then, in 1998, the State Council in France also emphasized this cooperation by stating that: “legislative and regulatory protection does not in itself allow reaching a satisfactory situation. It is important to involve professionals, especially the companies in the development of instruments to ensure the consumer rights” (Sarr,

2012, p. 56). So the cyberspace has allowed the interference of the non-state actors at the expense of state institutions and this has compromised the power of the state.

However, in cases of national security, governments are usually reluctant to leave matters in the hands of non-governmental organizations to regulate and deal with cyberspace activities, such as cyber wars and cyber-attacks which may cripple networks in strategic areas, for example, a few days after the start of military operations in Mali, France has been the target of cyber-attacks launched by hackers. As a result of these attacks, many French experts drew the government attention to the weakness of protecting France against the cyber-attacks (Bourassi, 2013). Nowadays, the cyber-attacks can be horrible—with limited resources, a limited group of individuals could be able to damage strategic electronic systems of a state by a simple cyber-attack. The problem becomes much worse when countries become completely dependent on information and communication technology (ICT) and the internet. According to Gendron (2013) “These infrastructures have become high-value targets as well as more vulnerable to attacks” (p. 179), for example, in the current globalized market, countries conduct their international trading relying on cross-border supply chains and new technology. In addition, “protecting cyberspace is more complex than protecting physical and geographic domains” (Gendron, 2013, p. 179).

In explaining the nature of the cybercrime and cross-border offending, Grabosky (2004, p. 146) outlined three typical activities that may undermine the sovereignty of the state: conventional crimes committed with computers (e.g., digital child pornography, piracy, or intellectual property theft, and forgery); attacks on computer networks; and conventional criminal cases (e.g., drug trafficking in which evidence exists in digital form). In addition, Matusitz (2008) referred to the potential of cyber-terrorism to create a postmodern state of chaos. Again, Alonso (2013) has pointed out the major economic burden that these cyber activities can cause. The state will spend a great deal of money in securing and protecting its network systems against potential cyber-attacks. The significance of cyber damage was referred to be Alonso (2013) explaining: “The spectre of cyber war develops from the most superficial level to the most sophisticated level, from state to state” (p. 6).

Conclusions

Since the formation of the state, sovereignty is considered as an essential component of the state. Thus, the state has endeavoured to maintain its sovereignty over its territories and has sought to protect its geographical boundaries by all possible means to prove its identity. However, technological revolution, including the telecommunication advancements, imposed new challenges to the state’s sovereignty in maintaining its cyber space.

Controversial views have debated the reality of cyberspace. On one hand, some researchers pointed out the concept of cyberspace as a libertarian fantasy that does not describe a real thing. On the other hand, other views have regarded cyberspace as a true international space, and therefore, any dispute related to cyberspace activities should be subjected to cyber-jurisdictions.

This paper argues that, regardless of cyberspace being a “libertarian fantasy” or a “true international space”, the common characteristics of cyberspace are that it is cross-border and poured. This makes the traditional means ineffective to protect the sovereignty and borders of the state.

Also, the research shows that cyberspace with its characteristics (dematerialization, detemporalization, and deterritorialazation) can cross borders and the territory of the state despite all the precautions taken by the state to protect its sovereignty. These characteristics make national laws unable to keep up to date with technological

developments. Yahoo, Google, and miditext.com case studies, discussed in this article, support this argument.

Consequently, states should look for new means to regulate the cyberspace, such as soft law. Therefore, legislators and regulators must be more flexible by giving an important role to the civil actors in regulating the cyberspace and the e-commerce issues. In this way, the state can reserve the framework powers or constitutional prerogatives.

References

Alonso, P. (2013). *Internet, another Syrian civil war*. Retrieved from http://www.slate.fr/story/69519/syrie-internet-hacking (Accessed 15 January 2015)

Bellanger, P. (2011). From sovereignty in general to digital sovereignty in particular. *In Les Echos.fr, 54*(30). Retrieved from http://lecercle.lesechos.fr/entreprises-marches/high-tech-medias/internet/221137239/souverainete-general-et-souverainete-numeriq (Accessed 28 February 2012)

Biegel, S. (2001). *Beyond our control? Confronting the limits of our legal system in the age of cyberspace*. London: MIT Press.

Bourassi. (2013). *Cyberwar, how France protects itself*. Retrieved from http://www.latribune.fr/entreprises-finance/industrie/aeronautiquedefense/20130111trib000742055/cyberguerre-comment-la-france-se-protege.html (Accessed 2 December 2014)

Brenkert, G. (2009). Google, human rights, and moral compromise. *Journal of Business Ethics, 85,* 453-478.

Chaffey, D., & Ellis-Chadwick, F. (2012). *Digital marketing: Strategy, implementation and practice.* London: Pearson.

Choucri, N., & Clark, D. (2013). Who controls cyberspace? *Bulletin of the Atomic Scientists, 69*(5), 21-31.

Cohen-Almagor, R. (2012). Freedom of expression, internet responsibility, and business ethics: The Yahoo Saga and its implications. *J Bus Ethics, 106,* 353-365.

Cruquenaire, A., & Lazaro, C. (2013). *The law applicable to international contracts concluded via Internet: The Rome convention*. Retrieved from http://www.crid.be/pdf/public/4049.pdf (Accessed 17 November 2014)

Deibert, R., Rohozinski, R., & Crete-Nishihata, M. (2012). Cyclones in cyberspace: Information shaping and denial in the 2008 Russia-Georgia war. *Security Dialogue, 43*(1), 3-24.

Duplessis, I. (2007). Vertigo and soft law, doctrinal reactions in international law. *Quebec Journal of International Law, Special Issue (Hors-série),* 245-268. Retrieved from http://www.crimt.org/PDF/hs07_duplessis.pdf (Accessed 02 February 2014)

Gendron, A. (2013). Cyber threats and multiplier effects: Canada at risk. *Canadian Foreign Policy Journal, 19*(2), 178-198.

Grabosky, P. (2004). The global dimension of cybercrime. *Global Crime, 6*(1), 146-157.

Grewlic, K. (1999). Good governance in the age of cyberspace. *The Journal of Policy, Regulation and Strategy for Telecommunications, 1*(3), 264-270.

Grosso, A. (2001). Domis of sovereignty. *Communications of the ACM, 44*(3), 102-104.

Hartnett, S. (2011). Google and the "Twisted Cyber Spy" Affair: US-Chinese communication in an Age of Globalization. *Quarterly Journal of Speech, 97*(4), 411-434.

Hassan, R. (2003). Network Time and the new knowledge epoch. *Time & Society, 12*(2/3), 225-241.

Hassan, R. (2009). *Empires of speed: Time and the acceleration of politics and society*. Leiden: Brill.

Hedley, S. (2003). Nations, markets and other imaginary places: Who makes the law in cyberspace? *Information & Communications Technology Law, 12*(3), 215-224.

Jacquot, F., & Weitzel, B. (2001). Litigations regulation. *The Legal Guide of Electronics Traders (Version Préliminaire),* 204-243. Retrieved from https://lexum.com/sites/default/files/publications/2001-guide-juridique-commercant-electronique.pdf (Accessed 5 June 3013)

Kobrin, S. (1997). Electronic cash and the end of national markets. *Global Issues, 2*(4), 38.

Kohl, U. (2007). *Jurisdiction and the Internet: A study of regulatory competence over online activity*. Cambridge: Cambridge University Press.

Kucklich, J. (2009). Virtual worlds and their discontents precarious sovereignty, governmentality, and the ideology of play. *Games and Culture, 4*(4), 340-352.

Laguerre, M. (2004). Virtual time, in information. *Communication & Society, 7*(2), 223-247.

Lee, H., & Sawyer, S. (2010). Conceptualizing time, space and computing for work and organizing. *Time Society, 9,* 293-316.

Levy, M. (23 May 2000). French Court says Yahoo broke racial law. *New York Times*, p. 4. Retrieved from http://www.nytimes.com/2000/05/23/business/french-court-says-yahoo-broke-racial-law.html

Lewis, J. (2010). Sovereignty and the role of government in cyberspace. *The Brown Journal of World Affairs, 16*(2), 55-65.

Lin, H. (2012). A virtual necessity: Some modest steps toward greater cybersecurity. *Bulletin of the Atomic Scientists, 68*(5), 75-87.

Maljean-Dubois, S. (2003). *Enforcement of international environmental law*. Retrieved from http://www.peacepalacelibrary.nl/ebooks/files/337934460.pdf (Accessed 18 March 2014)

Matusitz, J. (2008). Cyberterrorism: Postmodern state of chaos. *Information Security Journal: A Global Perspective, 17,* 179-187.

Matusitz, J. (2014). Intercultural perspectives on cyberspace: An updated examination. *Journal of Human Behaviour in the Social Environment, 24*(7), 713-724.

McGuffin, C., & Mitchell, A. (2014). On domains: Cyber and the practice of warfare. *International Journal, 69*(3), 394-412.

Mihalache, A. (2002). The Cyber Space—Time continuum: Meaning and metaphor. *The Information Society, 18,* 293-301.

Placid, R., & Wynekoop, J. (2011). Tracking the footprints of anonymous defamation in cyberspace: A review of law and technology. *Journal of Information Privacy and Security, 7*(1), 3-24.

Sarr, M. (2012). Soft law and electronic commerce. *Jurisdoctoria, 8,* 49-73. Retrieved from http://www.jurisdoctoria.net/pdf/numero8/NUMERO_8.pdf (Accessed 24 August 2014)

Schneider, G. (2013). *E-Business* (10th ed.). London: Course Technology, Cengage Learning.

Schultz, T. (2004). Online dispute resolution: Challenges for contemporary justice. *Kluwer Law International.*

Sheldon, J. (2014). Geopolitics and cyber power: Why geography still matters, in American foreign policy interests. *The Journal of the National Committee on American Foreign Policy, 36*(5), 286-293.

Tan, J. (2012). Business under threat, technology under attack, ethics under fire: The experience of Google in China. *J Bus Ethics, 110,* 469-479.

Thrift, N. (2006). Space. *Theory Culture Society, 23,* 139-146.

Wynn, E., & Katz, J. (1997). Hyperbole over cyberspace: Self-presentation and social boundaries in internet home pages and discourse. *The Information Society, 13,* 297-327.