BALTIC JOURNAL OF LAW & POLITICS
VOLUME 5, NUMBER 2 (2012)
ISSN 2029-0454
http://www.versita.com/science/law/bjlp

Cit.: *Baltic Journal of Law & Politics* 5:2 (2012): 132-163
DOI: 10.2478/v10076-012-0014-y

HOSTES HUMANI GENERIS: CYBERSPACE, THE SEA, AND SOVEREIGN CONTROL

Julija Kalpokienė

LL.M. student
School of Law, University of Nottingham (United Kingdom)

Contact information
Address: Law and Social Sciences Building, University Park, Nottingham NG7 2RD, United Kingdom
Phone: +44 115 951 5700
E-mail address: llxji3@nottingham.ac.uk

Ignas Kalpokas

Ph.D. student
School of Politics and International Relations, University of Nottingham (United Kingdom)

Contact information
Address: Law and Social Sciences Building, University Park, Nottingham NG7 2RD, United Kingdom
Phone: +44 115 951 4862
E-mail address: ldxik4@nottingham.ac.uk

Received: November 7, 2012; reviews: 2; accepted: December 28, 2012.

ABSTRACT

Cyberspace is a new global space that is yet not fully explored nor effectively regulated. The authors are not sketching a regulatory framework for cyberspace, but instead are inclined to glean valuable experience from the developments in the regulation of other global spaces, especially the sea. First, the peculiarities of cyberspace and cybercrime are briefly outlined. Then, the other global spaces are analysed drawing comparisons between exploration, appropriation and regulations of the sea and the air and cyberspace. The authors suggest that it is vital to learn lessons from the past in order to achieve an effective model of regulation of cyberspace. One of the main focus points of the paper is the position of a pirate and the ways of regulating piracy in different global spaces.

KEYWORDS

Cyberspace, cybercrime, sovereignty, regulation, cyber law, law of the sea

NOTE

The authors would like to thank the anonymous reviewers for their invaluable comments and suggestions. Also, a very kind thank you to Neil MacEwan for his inspirational Cyberlaw lectures at the University of Salford and guiding comments on an essay which was a start to this research.

INTRODUCTION

Cyberspace is relatively new, and the challenges of its regulation and law-enforcement are still difficult to tackle. This new global space is still very much unexplored. Because of its unique global nature, the problems in cyberspace are spanning beyond the jurisdiction of a sovereign state.

Despite the abundance of strategies and proposals, very little has been achieved as to universal agreement on cyberspace regulation. At the same time, there is a pressing need to regulate the cyberspace effectively because of its strategic importance, among other things, for the communications, businesses, governmental and non-governmental institutions, and, increasingly, the military. Thus, an effective regulatory framework is needed and for this end the specificities of cyberspace have to be understood and put in the wider context of different regulatory frameworks.

The authors argue that the nature and peculiarities of cyberspace and its possible regulation are best understood if compared to the other global spaces, especially with the sea. It is not the aim of this paper to sketch an alternative regulatory framework for cyberspace. However, it is submitted that by understanding the historical developments of the global spaces, the changes of their legal status and the philosophical as well as technological underpinnings of such changes, one would be able to learn from the past experience and potentially come up with more realistic and effective solutions for the regulation of cyberspace. Although the idea of treating cyberspace similarly to other global spaces has been raised as early as 1998,[1] such suggestions were more concerned with attempts to define jurisdiction over the space and to develop an effective nationality principle. More recent cyberspace regulation theories have discarded the quest for problematic territoriality principle in cyberspace favouring universal jurisdiction which often is inspired by the treatment of pirates in Maritime Law.[2] However, the attempts to place cyberspace in the family of the global spaces are rather occasional and tailored for specific purposes to discuss sporadic issues of cyberspace and/or cybercrime.

First part of the paper provides a brief overview of the nature of cyberspace, its uniqueness, cyber criminal activities and their problematic. In the second part a parallel between cyberspace and the sea is explored offering insights as to why

[1] Darrel C. Menthe, "Jurisdiction in Cyberspace: A Theory of International Spaces," *Michigan Telecommunications Law Review* 4 (1998).

[2] William M. Stahl, "The Uncharted Waters of the Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity," *Georgia Journal of International and Comparative Law* 40 (2011).

criminal activity flourishes in cyberspace. Also, potential challenges to regulation in cyberspace are outlined drawing on the experience of regulation of the sea. Then briefly, the regulation of the sea and the air is compared to better understand divergence of the two different global spaces' regulation. Such a comparison of regulatory frameworks of different global spaces may be of particular use drawing up cyberspace regulatory framework since cyberspace is yet another however new and not naturally formed global space which shares similar features with already explored and more regulated global spaces. Further the discussion will concentrate on two main themes: the figure of a pirate and the question of sovereignty in global spaces, particularly drawing on the sea. Crucial similarities between online and offline piracy will be pinpointed, employing the notion of Grotian emphasis and popularisation of the pirate as the 'enemy of the whole humankind', although the term *hostis humani generis* itself can be found as early as Cicero.[3] It is suggested that Grotius' book *Mare Liberum* offers relevant insights in modern cyberspace, because economic, political, and military issues were at stake in the context of the sea and the transformation of the pirate as they are now in cyberspace. Also, the problem of asserting jurisdiction and sovereignty over the sea and cyberspace will be analysed, paying special attention to technological developments and changes to the relative power of the most important states.

The authors suggest that the importance of the developments of the regulation of the sea offer valuable lessons that should not be overlooked when designing the regulatory framework of cyberspace not only because the sea also formerly was an unregulated space havening criminals, but also because appropriation and control are just as topical in modern cyberspace as they once were in the sea.

1. CRIME IN CYBERSPACE

Ironically, the internet which is essential for the existence of cyberspace was designed by the US military to be a secure system of communications that is not to be impeded by a nuclear attack.[4] Today, however, the internet is extensively used for civilian purposes. The early internet community was small and homogeneous operating in a collaborative spirit[5]; hence the design of the internet is rather not well suited for its currently diverse and pluralistic use adding to the security risks in

[3] Douglas R. Burgess, "Hostis Humani Generi: Piracy, Terrorism and a New International Law," *University of Miami International and Comparative Law Review* 13 (2006): 301.

[4] David Johnson and David Post, "Law and Borders – The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367.

[5] Vinton Cerf, Barry M. Leiner, David C. Clark, et al., "A Brief History of the Internet," *An International Electronic Publication of the Internet Society* (1997) //
http://www.isoc.org/oti/printversions/0797prleiner.html (accessed December 17, 2012).

cyberspace.[6] The regulation of cyberspace and fight against cybercrime has to overcome the problems that stem from the early days of the creation of the internet.

The domestic attempts to fight cybercrime differ from state to state. Also, academic suggestions vary from offers to regulate cyberspace in the same way as real space is regulated[7] (inherently problematic due to the difficulty of asserting jurisdiction and enforcing the law online) to creating a new self-regulatory system of cyberspace[8] since the terrestrial regulation lacks legitimacy and enforceability.[9] The latter is often compared to the Medieval *lex mercatoria*, the Law Merchant,[10] or to customary international law.[11] However, the *sui generis* nature and extensive homogeneity of the Medieval merchant law has recently been seriously challenged[12] while the customary law analogy fails to pinpoint who are the relevant actors whose custom is to be taken into account. Finally, one of the most grandiose propositions is the creation of a global cyber security system and an international cyber court.[13] While such solution would most probably solve the problem of jurisdiction, the willingness of states to commit to such an institution appears to be doubtful.

1.1. CYBERSPACE AND CYBERCRIME

One has to be aware of the unique nature of the cyberspace. Despite of the presence of what Yar calls the 'recognizable geography', i.e. the application of references to space and place, such as 'portals', 'sites', 'cafes', 'classrooms', etc.,[14] cyberspace is fundamentally new. Perplexingly, there is no single all-encompassing definition of cyberspace. The Advocate General Cruz Villalon at the European Court of Justice has recently described cyberspace as one which has transformed the spatial and territorial conception of communications and thus has created an intangible or even ungraspable space which has no limits or frontiers enabling the transfer of information immediately with the potency of storing the information

[6] Jose MA. Emmanuel Caral, "Lessons from ICANN: Is the Self-regulation of the Internet Fundamentally Flawed?" *International Journal of Law and Information Technology* 12 (1) (2004): 28.

[7] Chris Reed, "Online and Offline Equivalence: Aspiration and Achievement," *International Journal of Law and Information Technology* 18 (3) (2010): 248.

[8] Graham Greenleaf, "Regulating Cyberspace: Architecture vs Law?" *The University of New South Wales Law Journal* 21 (2) (1998): 602.

[9] Davi Johnson and David Post, *supra* note 4: 1375.

[10] *Ibid.*: 1389-1390.

[11] Warren B. Chik, "'Customary Internet-tional Law': Creating a Body of Customary Law to Cyberspace. Part 1: Developing Rules for Transitioning Custom into Law," *Computer Law & Security Review* 26 (2010): 4.

[12] Emily Kadens, "The Myth of the Customary Law Merchant," *Texas Law Review* 90 (5) (2012): 1153-1206.

[13] Nicholas W. Cade, "An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code," *Brooklyn Journal of International Law* 37 (3) (2012).

[14] Majid Yar, "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory," *European Journal of Criminology* 2 (2005): 415.

forever.[15] A more technological definition by the US Department of Defence states that the cyberspace is a 'global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers'.[16] Cyberspace is also named a 'new Wild West' where criminals find a virtual haven; however, the victims are real.[17] Unlike the real world where borders of sovereign states restrict movement, the cyberspace is borderless without any guidance or 'signposting' of applicable law to certain place in the space.[18] In addition, cyberspace is described as 'an electronic sea of thought expressed in text, image, and sound.'[19] At its core is the possibility of unlimited information exchange by unlimited subjects between unlimited places.[20] Others, meanwhile, would prefer not to dwell into the specificity of cyberspace perceiving it not as a new space but rather as a natural extension of globalisation, albeit in a virtual dimension, which had existed even before the technological capacity to access it.[21] However, such views are clearly in a minority.

The European Commission defines cybercrime as 'criminal acts committed using electronic communications networks and information systems or against such networks and systems'.[22] The term 'cybercrime' is used to define the crimes committed or facilitated by the use of digital technologies and includes both already existing crimes, for example, fraud or child pornography, and also activity that is targeted at the technology itself, thus crimes that are possible only because of the existence of the technology[23] (for example, spamming or Distributed Denial of Service (DDoS) Attacks). However, the difficulty arises in defining and classifying cybercrime because of uncertainty of who the perpetrators are and what their affiliation is: whether they are linked with a criminal organisation or sponsored by a sovereign state.[24] Therefore, it is obvious that cybercrime is a multi-faceted

[15] *eDate Advertising GmbH v X (C-509/09) and Olivier Martinez and Robert Martinez v MGN Limited (C-161/10)*, European Court of Justice, Opinion of Advocate General Cruz Villalon (March 29, 2011), para. 43.

[16] Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms, "Joint Publication 1-02" (2001) // http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed November 4, 2012).

[17] Natasha Jarvie, "Control of Cybercrime – Is an End to Our Privacy on the Internet a Price Worth Paying? Part 1," *Computer and Telecommunications Law Review* 9 (3) (2003): 76.

[18] David Johnson and David Post, *supra* note 4: 1368.

[19] Mark Frazzetto, "A Maritime Model for Cyberspace Legal Governance," *The National Strategy Forum Review* (September 19, 2011) // http://nationalstrategy.wordpress.com/ (accessed November 4, 2012).

[20] Bernhard Maier, "How Has the Law Attempted to Tackle the Borderless Nature of the Internet?" *International Journal of Law and Information Technology* 18 (2) (2010): 143.

[21] Georgios I. Zekos, "Globalisation and States' Cyber-Territory," *Web Journal of Current Legal Issues* 5 (2001).

[22] *Towards a General Policy on the Fight against Cyber Crime*, the Council and the Committee of the Regions, Communication from the Commission to the European Parliament (COM/2007/0267 final) {SEC(2007) 641} {SEC(2007) 642}.

[23] Jonathan Clough, "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data," *Criminal Law Forum* 22 (1) (2011): 150.

[24] William M. Stahl, *supra* note 2: 270.

phenomenon connected by a thin thread of technology used rather than being a particular type of offending.[25]

Each global space has its own peculiarities, and cyberspace is not an exception. Most importantly, the non-physical character of cyberspace brings crucial transformations to criminal acts committed in this space and hinders the efforts to tackle them. Four distinctions of cybercrimes from terrestrial crimes can be made: it is easy to learn how to commit a crime in cyberspace, relatively few resources are needed for the commission of a crime compared to the damage it causes, cybercrime can be committed from any jurisdiction in any jurisdiction without physically being there, and often such crimes are 'not clearly illegal'[26] as there is no clear 'signposting' of jurisdictions in cyberspace and also while an act is illegal in one jurisdiction, it might be not outlawed in another. For example, holocaust denial is a crime in France whereas in the USA it is not and, as it was in Yahoo case,[27] the government might choose to prosecute an entity for providing access to the citizens to prohibited material. Cybercrimes can affect people around the globe, spread in the matter of minutes or hours, and it is hard to estimate the harm inflicted by such crimes.[28] Contrastingly, terrestrial crimes are confined to the locality and normally are restricted by state borders. Also, they are small-scale and tend to be personal. Thus, the apprehension of offenders is relatively easy compared with cybercriminals who act globally without any restrain of sovereign states' borders. Moreover, criminal activity in cyberspace has the potential to spread around the globe quicker than anything before.[29]

1.2. SUPPLY OF CRIMINALS AND OPPORTUNITIES TO OFFEND

Piracy has always been an issue where effective control was lacking: in the high seas and in territories where local government is weak and unable to enforce order, a recent example being an upsurge in piracy off Somalia.[30] This is also true for cybercrime which flourishes not only due to the lack of control but also due to the unwillingness or inability of some states to tackle it within their own jurisdiction.[31] Indeed, very often states have no means, expertise and/or finance to tackle cybercrime effectively or simply have other priorities, such as economic

[25] Jonathan Clough, "Cybercrime," *Commonwealth Law Bulletin* 37 (4) (2011): 672.

[26] Susan W. Brenner and Marc D. Goodman, "The Emerging Consensus on Criminal Conduct in Cyberspace," *International Journal of Law and Information Technology* 10 (2) (2002): 143.

[27] *League Against Racism and Antisemitism (LICRA), French Union of Jewish Students v Yahoo! Inc. (USA), Yahoo France*, Tribunal de Grande Instance de Paris (The County Court of Paris), Interim Court Order (November 20, 2000), Electronic Business Law Reports 1 (3) (2001).

[28] Jonathan Clough, *supra* note 25: 141.

[29] *Ibid*.: 152.

[30] Douglas Guilfoyle, "Piracy off Somalia: UN Security Council Resolution 1816 and IMO Regional Counter-Piracy Efforts," *International Criminal Law Quarterly* 57 (2) (2008): 691.

[31] Susan W. Brenner and Marc D. Goodman, *supra* note 26: 139.

development or tackling widespread terrestrial crime, which usually poses a greater immediate threat.[32] Still other states may secretly support cybercriminals or cyber terrorists if they are seen to further the state's strategic aims.[33]

The motivation to commit offences in cyberspace varies, and the motives include revenge which could be against anyone from person to country or even continent, financial gain, curiosity, and fame. The latter two can be particularly strong drives that are often disregarded. In reality, it is adventure, the exploration of the unknown that attracts a lot of people.[34] Also, strive for fun, intellectual stimulation, or sexual drive could foster commission of criminal acts in cyberspace.[35] Furthermore, there is a tendency that people treat cyberspace differently from the real space and often perceive it to have lower standards of behaviour. This is evident in intellectual property breaches in cyberspace, and many people who normally would not, for example, copy a compact disc for a friend, in cyberspace do infringe copyright engaging in file sharing.[36] Finally, the commission of criminal acts is much easier in cyberspace. There is no need to travel in order to carry out a criminal act, and at once many victims can be targeted easily and quickly.[37] Also, there are different tools that are on offer for sale to facilitate or even to carry out a criminal act online effortlessly and without any prior knowledge.[38] After all, cyberspace is perceived as enabling anonymity.[39] Moreover, statistics suggest that people turn to cybercrime for living, because it is relatively easy to commit a crime and cover up the traces and the apprehension is perceived as low risk.[40]

There are numerous reasons why cyberspace offers more opportunities to offend than physical space. First of all, there are no frontiers in cyberspace, thus the barriers are lacking to stop one from offending. Artificial borders can be introduced by national or supranational regulations but they are rarely effective. Easy access to a pool of potential victims is a tempting feature of cyberspace.[41] Closely related is the ability to affect multiple locations around the world (or the entire globe itself) from one particular location, however remote.[42] Or, conversely, it is not rare that an attack that at first appeared to have taken place from a distant

[32] Peter Grabosky, "The Global Dimension of Cybercrime," *Global Crime* 6 (1) 2004: 152.
[33] Alexander Klimburg, "Mobilising Cyber Power," *Survival: Global Politics and Strategy* 53 (1) (2011): 42.
[34] Peter Grabosky, *supra* note 32: 149-150.
[35] Bert-Jaap Koops, "The Internet and its Opportunities for Cybercrime": 735; in: M. Herzog-Evans, ed., *Transnational Criminology Manual* (Nijmegen: Wold Legal Publishers, 2010).
[36] Chris Reed, *supra* note 7: 253.
[37] Susan W. Brenner and Marc D. Goodman, *supra* note 26: 152.
[38] Jonathan Clough, *supra* note 25: 673.
[39] Natasha Jarvie, *supra* note 17: 76.
[40] Susan W. Brenner and Marc D. Goodman, *supra* note 26: 144.
[41] Majid Yar, *supra* note 14: 415.
[42] Bernhard Maier, *supra* note 20: 174.

location, was, as a matter of fact, committed from next door via remote servers.[43] Thus new possibilities for cybercriminals to hide their traces are offered. Also, the ease of building up an army of bots that can be used for criminal activities enable one to exploit other unknowing and innocent people to carry out a criminal act.[44] Cybercrime also enjoys an unprecedented scale as nowhere else there is such a high number of victims and lucrative targets which can be reached without physically travelling.[45] Moreover, identification of the offender is difficult because of the nature of commission of cybercrime: it is relatively easy to trace the origins of the crime but much more complicated to identify the offender himself.[46] It can be said that the internet has eliminated borders – and the applicability of national law with them – to an unprecedented extent.[47]

Especially, with no effective global law governing cyberspace, and the difficulties associated with prosecuting criminals because of the jurisdictional limits, it is difficult to identify, catch, and put to trial the offenders who operate in cyberspace.[48] These jurisdictional limits order the absence of unified legal definitions of crimes (certain acts in cyberspace are not globally outlawed) and inherently the states are often unable to prosecute offenders that are beyond their reach. Moreover, usually it is impossible to clearly determine where a crime originated from because the crime scene is virtual.[49] What is more, even when regulation is available either on national or supranational level, the sheer pace of technological advancement and thus the development of new crimes becomes an issue as it threatens to outpace the attempts to define emerging crimes.[50] Finally, the property that is in cyberspace is intangible thus easily and conveniently transportable once accessed but nevertheless might be extremely valuable.[51] The opportunities to offend in cyberspace are vast as the cyberspace itself and, moreover, are being developed together with the new technologies.

1.3. LACK OF CAPABLE GUARDIANS

The interconnectedness of the terrestrial space and the cyberspace is problematic: while it is indeed true that actions in the latter have clear consequences in the former,[52] it is not necessarily true the other way round. As a

[43] Peter Grabosky, *supra* note 32: 150-151.
[44] Jonathan Clough, *supra* note 25: 676.
[45] *Ibid.*: 673.
[46] Majid Yar, *supra* note 14: 421.
[47] Bernhard Maier, *supra* note 20: 143.
[48] Jonathan Clough, *supra* note 25: 674.
[49] Natasha Jarvie, "Control of Cybercrime – Is an End to Our Privacy on the Internet a Price Worth Paying? Part 2," *Computer and Telecommunications Law Review* 9 (4) (2003): 112.
[50] Jonathan Clough, *supra* note 25: 671.
[51] Majid Yar, *supra* note 14: 420.
[52] Georgios I. Zekos, *supra* note 21.

result, the attempts of terrestrial actors to regulate cyberspace activities have enjoyed rather limited success. First and foremost, this is because the virtual space resists any territorial principle. Even if national courts have their say in cybercrime cases, these decisions are not necessarily possible to implement without international cooperation.[53] Therefore, a greater harmonisation is needed, but an agreement of many actors is always much more difficult to achieve.

The most significant international agreement tackling the challenges of cybercrime is the Council of Europe's Convention on Cybercrime[54] that came into force on 1 July 2004 and also is signed by a number of non-member states such as Canada and the United States (US).[55] However, it is often difficult to draw up an international agreement on cybercrime, because there are disagreements between the states which activities actually should be included in the definition of cybercrime.[56]

Also, there are two differing positions in international arena of regulating cyberspace: China and Russia are advocating the state-led international framework, in which more control over the cyberspace should be allocated to sovereign states and inter-state organisations, e.g. United Nations (UN) bodies, whereas Western democracies are for a more libertarian *laissez faire* model with a multi-stakeholder approach including not only states but businesses as well.[57] These two positions appear to be impossible to reconcile in the near future. It could be argued that China is in favour of the state led international framework because of its strive to retain its social order and stability,[58] Russia’s position could be interpreted as a counter-hegemonic struggle: an attempt to limit the influence of other powerful states in the area which Russia cannot control itself. The multi-stake holder approach supported by the Western democracies seems natural because the majority of proposed stakeholders are situated in those states. For example, The Internet Corporation for Assigned Names and Numbers (ICANN), one of the core organisations that oversee the Internet which would naturally form part of the stakeholders in the multi-stake holder framework, is incorporated under the US laws.[59] Most recently, the disagreements on the right model to regulate cyberspace were exposed at the 2012 World Conference on International Telecommunications

[53] Bernhard Maier, *supra* note 20: 147.
[54] *Convention on Cybercrime*, Council of Europe, CETS No. 185 (Budapest; November 23, 2001).
[55] Jonathan Clough, *supra* note 25: 152.
[56] Susan W. Brenner and Marc D. Goodman, *supra* note 26: 144.
[57] Henry L. Judy and David Satola, “Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?” *Business Law Today* (December 2011) // http://apps.americanbar.org/buslaw/blt/content/2011/12/article-2-judy-satola.shtml (accessed November 4, 2012).
[58] Uchenna Jerome Orji, “An Analysis of China’s Regulatory Response to Cybersecurity,” *Computer and Telecommunications Law Review* 18 (7) (2012): 213.
[59] Franz C. Mayer, “The Internet and Public International Law – Worlds Apart?” *European Journal of International Law* 12 (3) (2001): 61.

in Dubai. Although one of the aims of the Conference was to confer more Internet regulation powers to the International Telecommunication Union (ITU),[60] the issues discussed at the Conference were not of core importance to cyber security. Once again, the states promoting state-led Internet regulation framework failed to get the support of multi stake-holder approach supporters failing to agree what content on the Internet should be controlled.[61]

Another issue is the difficulty of prosecuting cyberspace offenders under domestic law in absence of cybercrime legislation. For example, in property offences it has to be relied on existing property laws and this poses problems when computer data is in question: traditional concept of property does not apply if, for example, the data was not modified but merely accessed.[62] Also, a question arises as to which units of cyberspace environment are to be regulated: cyberspace as a whole or just a definite list of elements that make up the 'greater picture' (for example, 'cookies', banners, applications, etc.).[63] The first perspective means significant risk of diminishing freedom online. The second, meanwhile, risks to be outpaced by rapid developments in cyberspace.

There are even more aspects that contribute to the lack of capable guardians in preventing criminal activity in cyberspace: first, the space is so vast that it is virtually impossible to police it all (combining crime prevention, interception of an ongoing criminal activity and investigation).[64] Secondly, social norms formed in cyberspace are important in shaping behaviour there.[65] As already mentioned, people often perceive the standards of behaviour to be lower in cyberspace, and thus it is impossible to enforce something that is thought to be morally right by the masses. Thirdly, although governments can pressure software development companies, internet service providers and other major actors that are within their jurisdiction to implement anti-cybercrime measures, such controls are not necessarily effective due to the global interconnectedness of cyberspace.[66] Also, the self-regulatory cyberspace governance poses problems not only because the

[60] John Blau, "Battle Brewing over International Internet Regulation," *IEEE Spectrum* (December 2012) // http://spectrum.ieee.org/telecom/internet/battle-brewing-over-international-internet-regulation (accessed December 26, 2012).

[61] "Conference Concludes in Dubai with 89 Countries Having Signed the Updated International Telecommunication Regulations," *World Conference on International Telecommunications Highlights* (December 13-14, 2012) // http://www.itu.int/osg/wcit-12/highlights/dec13-14.html#.UNrqWW_brE1 (accessed December 25, 2012); Jennifer Scott, "ITU Internet Regulation Blocked by UK and US," *ComputerWeekly.com* (December 14, 2012) // http://www.computerweekly.com/news/2240174668/ITU-regulation-blocked-by-UK-and-US (accessed December 26, 2012).

[62] Jonathan Clough, *supra* note 23: 150-151.

[63] Bernhard Maier, *supra* note 20: 161.

[64] Majid Yar, *supra* note 14: 423.

[65] *Ibid*.: 423.

[66] Jose MA. Emmanuel Caral, *supra* note 6: 3.

effectiveness of such model is questionable (who would enforce the rules?) but its legitimacy and what or who is the 'self' are ambiguous.[67]

Every interested party be it states, right owners, or law enforcement agencies argue for more regulation in favour of the protection of their causes, however, if all the regulations are implemented without being duly considered, cyberspace risks to become a very restricted and censored space and not functional anymore, because its very essence comes from its multilayer nature and there is no supreme regulatory body that would overlook the control of it all.[68]

All in all, although there is no clearly effective way of fighting cybercrime, it is evident that protection against cybercriminals often requires more financial resources and technological expertise than prevention of conventional crime. Such resource demand puts states with lower economical capacity in an extremely disadvantaged position because, having to protect the entire civil and military infrastructure as well as the whole population, they cannot compete in the market for the most skilled professionals whose services are in demand by private businesses, states and criminals.[69]

2. THE THREE GLOBAL SPACES

Cyberspace is not entirely unique in its lack of borders and regulation: the sea and the air are the earlier (already appropriated) global spaces.[70] Therefore, a parallel between cyberspace and the sea can be illustrative. It is noteworthy that the advocates of freedom in cyberspace often ground their ideas on the Grotian doctrine of the freedom of the sea. Also, certain illegal activities in cyberspace are named as 'piracy'.[71] It is no coincidence that the current official definition of piracy includes illegal acts involving both ships and aircraft[72] – the vessels operating in the two global spaces.

2.1. THE APPROPRIATION OF THE SEA

An important insight into the nature of the sea and piracy is offered by a controversial German theorist Carl Schmitt. He notes that the word 'pirate' is

[67] *Ibid*.: 4.

[68] Wolfgang Kleinwachter, "Internet Governance Outlook 2012: Cold War or Constructive Dialogue," *Communications Law* 17 (1) (2012): 14.

[69] Toomas Hendrik Illves, "It's the Economy, Stupid!" *The Security Times* (September 2012): 24.

[70] Sumit Ghosh and Elliot Turrini, *Cybercrimes: A Multidisciplinary Analysis* (Heidelberg: Springer, 2010), p. 336.

[71] Mitchell Dean, "Nomos: Word and Myth": 242; in: Louiza Odysseos and Fabio Petito, eds., *The International Political Thought of Carl Schmitt: Terror, Liberal War, and the Crisis of Global Order* (Abingdon and New York: Routledge, 2007), p. 252.

[72] Tullio Treves, "Piracy, Law of the Sea, and Use of Force: Developments off the Coast of Somalia," *European Journal of International Law* 20 (2) (2009): 401.

derived from the Greek *peiran*, which means 'to try' or 'to test' and has originally signified an adventurer, often a noble one.[73] The adventurous nature stems from a fundamental difference between land and sea: land can be divided and fenced, and it has to be cultivated for production thus being bound by spatially defined order and law. Therefore, 'the earth is bound to law in three ways. She contains law within herself, as a reward of labor; she manifests law upon herself, as fixed boundaries; and she sustains law above herself, as a public sign of order'.[74] None of this applies to the sea: no firm lines can be fixed, and ships can sail as far as natural conditions allow them without leaving any durable trace; also, the riches of the sea are accessible without cultivation, even if accessing them does involve human labour; as a result, there was no law on the sea.[75] For example, according to one of the most authoritative figures in Medieval legal thought[76] Isidore of Seville '[i]nternational law is land-appropriation, building cities and fortifications, wars, captivity, bondage, return from captivity, alliances and peace treaties, armistice, inviolability of envoys, and prohibition of marriage with foreigners.'[77] Notably, nothing regarding the sea was mentioned because the sea was perceived as beyond the relations between people and nations. Land and sea were simply incommensurable and the traditional notions of *imperium* and *dominium* that characterised pre-modern sovereignty simply did not apply.[78] The sea also was a source of fear and mystery – as a notable example, the Apocalypse of Saint John states that there will be no more oceans when the earth is purged of sins[79] and the maps of a flat earth usually portrayed it as surrounded by water as the ultimate limit. This can also be said of the modern image of the cyberspace: it is seen as astonishingly liberating and horrifyingly full of sin and danger at the same time.

The sea was not only an anomic space – it was a frontier that separated the known and the ordered world from the unknown one where laws did not apply. As a result, even after the sea and the land beyond it were appropriated (or at least appropriation attempts were made) there was no equality of legal status between the European mainland states and their overseas colonies, because the latter were an 'outer space' beyond the sea.[80] The liminal nature of the sea as a borderline between two separate worlds was only eradicated in the modern era (first and

[73] Carl Schmitt, *The Nomos of the Earth in the International Law of Jus Publicum Europaeum* (New York: Telos, 2003), p. 43.
[74] *Ibid*., p. 42.
[75] *Ibid*., p. 42-43
[76] Oliver O'Donnovan and Joan Lockwood O'Donnovan, "Isidore of Seville": 204; in: Oliver O'Donnovan and Joan Lockwood O'Donnovan, eds., *From Irenaeus to Grotius: A Sourcebook in Christian Political Thought, 100-1625* (Grand Rapids and Michigan: William B Eerdmans Publishing, 1999).
[77] Isidore of Seville, *c.f.* Carl Schmitt, *supra* note 73, p. 44.
[78] David Armitage, "The Elephant and the Whale: Empires of Land and Sea," *Journal for Maritime Research* 9 (1) (2007): 30.
[79] Carl Schmitt, *supra* note 73, p. 43.
[80] Walter Prescott Webb, *The Great Frontier* (Reno: University of Nevada Press, 2003), p. 334.

foremost due to the new means of warfare, transport and communication). As a result, there is a notable difference between the sea and the cyberspace as the latter has from the very beginning been perceived a space of communication and not as a frontier.

The sea had not even approached a state of being appropriated until the great geographical discoveries when the great maritime powers have transformed it into a limitless trade route, but even then only a very limited control could be exerted over the sea. At the beginning, there were two paths that the treatment of the sea could take, one leading to a closed and the other to an open nature of the sea. These paths were evident in the first two global lines that divided the seas and the lands beyond them: the Spanish–Portuguese *rayas* (the divisions of the sea between Portugal and Spain), drawn in the Treaty of Tordesillas in 1494, and the French–English 'amity lines' of the Cateau-Cambrésis treaty drawn in 1559. Both of them signalled a new world order after new vast territories had been opened for appropriation by new geographical discoveries. The difference between the two is, nonetheless, fundamental: the *rayas* had a distributive purpose (i.e. division of territories between two princes), while the 'amity lines' were primarily *agonal* (i.e. they delimited spaces which were already appropriated from those open for contestation where force could be freely used).[81] The *rayas* signified an intention to control: first and foremost to control the land beyond the seas, but also, even if as a secondary effect, the seas themselves, because they were vital for control of the land as a military and cargo route. Therefore, the *rayas* were paradigmatic of the closed seas where water is an extension of territorial sovereignty. However, neither Portugal nor Spain was able to *de facto* exert and maintain control over the seas. Therefore, the later French-English 'amity lines' delimited the border between order, law and prognostication on 'this side' and *anomie* – disorder, anarchy and contingency which prevailed beyond the line either in the sea or on an unpartitioned, not yet appropriated land which was, in a way, an empty space.[82] On 'this side' of the line it was possible to make a decision which could establish and determine order for structuring relations between persons or political entities and thus creating an 'outer side' where no legal, moral or political order was possible. Hence 'outer side' is a permanent state of exception: first, a negative projection of 'inside'; second, it is an 'inside's' constitutive part in which all enmity is unleashed.[83] By definition there could be no real sovereignty beyond the 'amity

[81] Louiza Odysseos and Fabio Petito, "The International Political Thought of Carl Schmitt": 5; in: Louiza Odysseos and Fabio Petito, eds., *The International Political Thought of Carl Schmitt: Terror, Liberal War, and the Crisis of Global Order* (Abingdon and New York: Routledge, 2007).

[82] Michael Marder, *Groundless Existence: The Political Ontology of Carl Schmitt* (New York and London: Continuum, 2010), p. 21.

[83] *Ibid*., p. 22.

lines'. In addition, one has to keep in mind that the sea, although crucial in logistical terms, was never the core of any major power – even the English or the Dutch were first and foremost territorial land-based entities, despite the relative insignificance of their 'home' territory in comparison to the overseas colonies, settlements and dependencies.[84]

2.2. ATTEMPTS TO REGULATE THE SEA

Two prominent early examples of juridical attempts to conceptualise the status of the sea were those of Hugo Grotius and John Selden. Both attempts clearly illustrated the need to choose between the extremes of closed and free seas and the power interests that lay behind them. Grotius was employed by a trading company, and hence his theory of the free sea has to be understood in the light of the Dutch competition for trade routes.[85] His theory of the free sea, expressed in the treatise *Mare Liberum* (1609), was primarily a rebuttal of the Spanish and Portuguese claims to own the trade routes and an attempt to establish his employer's (equal) rights to trade and to extract the riches of the sea wherever they intended and saw fit to do so.[86] The Grotian doctrine of the free sea rested on two main principles: firstly, on the sea's immeasurable vastness which made it impossible to occupy control or exhaust the sea by navigation and fishing;[87] secondly, on the rights to travel and trade which were expressed in the Law of Nations.[88] The sea's fluidity, impossibility to confine it within fixed boundaries and its nature of facilitating exchange and interchange only confirmed the incommensurable difference between the land and the sea the latter being imagined as a common property of the entire humankind.[89] Such perception was clearly beneficial for the interests of the emerging maritime trading powers. It also reflected the changing power balance in Europe: the *rayas* were brokered by the Pope and Grotius being a Protestant not only did not feel bound to observe such an agreement, but also in a gesture characteristic to religious Reformation emphatically rejected any transcendent claim to earthly authority.[90]

The only serious attempt to challenge Grotius' view was that of Selden who, in *De Mare Clausum* (1635), argued in favour of a state's right to enclose certain parts of the sea and restrict the activities of others in order to protect its own strategic

[84] David Armitage, *supra* note 78: 26.

[85] Den Hartogh and Cees Maris, "The Commencement of Modern Age": 107; in: Cees Maris and Frans Jacobs, eds., *Law, Order and Freedom: A Historical Introduction to Legal Philosophy* (Heidelberg; Springer, 2011).

[86] James C. F. Wang, *Handbook on Ocean Politics and Law* (Westport: Greenwood Press, 1992), p. 75.

[87] *Ibid*., p. 75.

[88] Walter Prescott Webb, *supra* note 80, p. 333.

[89] David Armitage, *supra* note 78: 30.

[90] Arvid Pardo, "The Law of the Sea: Its Past and its Future," *Oregon Law Review* 63 (1) (1984): 10.

interests.[91] This, however, could be seen as a defensive strategy of a state not capable of dominance, i.e. an attempt to fence certain territories from the dominance of others. Although not particularly influential at that time, Selden's thought did gain some prominence later. In the meantime, however, it was the Grotian doctrine, albeit with minor modifications (notably, that of Cornelius van Bynkershoek that introduced the cannon-shot rule, i.e. the span of territorial waters necessary to protect coastal cities from bombardment from the sea[92]) that was more or less unanimously accepted.[93]

The Grotian doctrine of the free sea prevailed for around 300 years. First and foremost the doctrine was embraced by the main sea power of that time Great Britain which had abandoned Selden's views as soon as it had achieved the dominance of the seas, and later the US followed suit. However, as soon as the major maritime powers' support to the Grotian doctrine started to weaken, the system began to falter.[94] Indeed, the freedom of the sea was only possible either when there were no powers able to exert full sovereignty over the sea (the original Grotian solution) or one country was able to maintain the power over the sea and patrol it. The latter ability was also illustrated by the early formulation of the 2nd century Roman jurist Marcianus' doctrine of the freedom of the sea (Digest of Justinian, Book I Chapter VIII) which was based on the Rome's ability to control the Mediterranean Sea.[95] Upon the increase of the number of maritime powers increasingly able to compete with the Britons (primarily the likes of the US, Japan, and Germany), arose a need for a negotiated regulation and the law of the sea or otherwise a major conflict resulting in a division would be unavoidable.[96] Therefore, the principle of the free sea which before World War I appeared to be an irreplaceable principle, soon afterwards due to increasingly bold attempts to gain as much jurisdiction over the sea as possible marked a return to almost Selden-like strategies.[97] Evidently, a threat to security and/or vital interests of the states (and particularly the stronger and more influential ones) acts as catalysts to change the regulation(s) of the sea.[98] Importantly, it is *their (states')* particular interest and *their* reaction to *their* perceived threats that the states attempt to push forward as the universal means of regulation, especially as maritime security is an inclusive

[91] James C. F. Wang, *supra* note 86, p. 75-76.
[92] Wilhelm G. Grewe, *The Epochs of International Law* (Berlin: Walter de Gruyter, 2000), p. 328.
[93] Christopher L. Connery, "Ideologies of Land and Sea: Alfred Thayer Mahan, Carl Schmitt, and the Shaping of Global Myth," *Elements* 28 (2) (2001): 179.
[94] James C. F. Wang, *supra* note 86, p. 75-76.
[95] Arvid Pardo, *supra* note 90: 7.
[96] Christopher L. Connery, *supra* note 93: 182.
[97] Arvid Pardo, *supra* note 90: 12.
[98] Natalie Klein, *Maritime Security and the Law of the Sea* (Oxford and New York: Oxford University Press, 2011), p. 3.

need of all.[99] Therefore, the tension between an inclusive need and exclusive interest is paradigmatic to the regulation of a global space such as the sea (but also applicable to the air and cyberspace).

The tension between inclusive needs and exclusive interests is clearly visible in the changes of regulating the sea that occurred during the 20th century. As the economic and military interests of the states became increasingly global, more and more influence was claimed over large territories that earlier had been considered to be free.[100] The continental shelf doctrine aimed primarily at the ownership of natural resources, the Anglo-Norwegian Fisheries Case[101] in the International Court of Justice (ICJ) which limited the traditional freedom of economic enterprise, and the multiple failures to reach an agreement over the extent of territorial waters were the signals of the new partitions of the seas before a final settlement was reached with the UN Convention on the Law of the Sea in 1982.[102] Technological change could be seen as one of the most important reasons for the shifting attitude. The sea, albeit still vast and potentially dangerous, is no longer seen as immeasurable and impossible to effectively control, in a clear contrast with the time of Grotius. Also, the ability to exploit resources, often found in particular concentrated spaces and not in the entire sea in general (e.g. oil and gas) made sovereignty over at least some areas of the seas of paramount economical and military importance.[103] Furthermore, in a nowadays world which has been completely appropriated and which is increasingly imagined as populated by humanity rather than by particular nations, the existence of 'amity lines' that divide order and *anomie* is hardly imaginable. Therefore, global spaces such as the sea and the air (and, as it will be argued later, the cyberspace) have to be normalised and ordered and included into the everyday imagery in such a way as to reflect the economical and political developments and the power divisions that are present on the firm land.

2.3. COMPARING THE GLOBAL SPACES

If the two global spaces – the sea and the air – are compared, the air should be seen as much more divided than the sea. Under the current international law the airspace above a state's physical territory and above its territorial waters up to the limits of the atmosphere belongs to the sovereign domain of that state, which

[99] *Ibid*., p. 4.
[100] *Ibid*., p. 12-13.
[101] *Anglo-Norwegian Fisheries Case*, I.C.J. Reports 1951, 116.
[102] Klein, *supra note* 98: 13.
[103] *Ibid*.: 8.

makes sovereign territory three-dimensional.[104] There are good reasons for that: first of all, the air cannot be treated same as the open sea because of its potential military use. Historically, only a limited bombardment had been possible from the sea (and largely remains so, cruise missile submarines and aircraft carriers notwithstanding) while the air has a massive strategic importance. The sea does not overlap with the states' territory in the strict sense, except for the territorial waters (a bit more complicated with the cyberspace) while the air does. Boundaries cannot be drawn in the air but they are drawn on the land below.[105] The same ambivalent relation to borders, at least in theory, also applies to the cyberspace. Thus just as an illegal incursion into a state's airspace constitutes a violation of its sovereignty (regardless of the fact that these incursions, with or without pretext, have significantly increased in number in recent years[106]), the same applies to the cyberspace: illicit, illegal, and/or hostile activities by other states and non-state actors alike pose a significant threat to a state's interests and constitute a violation of its sovereignty by directly affecting its territorial domain. Notable examples of the latter could include cyber-attacks against Estonia in 2007, the publication of US diplomatic correspondence by "Wikileaks", or the Stuxnet virus, presumably targeted at Iran's nuclear capabilities. The presumably Russian-backed cyber attacks against Georgia during the 2008 South Ossetia war also serve as a notable example of coordinated cyber and ground warfare.

There are notable similarities between the early attitudes towards the air and the ongoing discussions about the regulation of the cyberspace. The advent of aviation, as the advent of cyberspace, was marked by discussions concerning aerial sovereignty and its applicability. There were those who backed the 'aerial trespass' rule claiming the air to be the property of each individual landlord while others assigned this dominion to states; there were also more than few who claimed the air to be completely free and borderless.[107] The 'sovereigntist' branch (which gained prominence after World War I) had illustrated the military capabilities of the new technology that could only be limited by the principle of state sovereignty. As a result, the first international civil aviation regime was established at the Paris Conference of 1919 and subsequently entrenched in the Chicago Convention on

[104] Alison J. Williams, "A Crisis in Aerial Sovereignty? Considering the Implications of Recent Military Violations of National Airspace," *Area* 42 (1) (2010): 51-52.

[105] Admittedly, there are occasions when land borders and the control of airspace do not strictly coincide, because some states may control parts of their neighbours' airspace if international agreements provide so. The case of the northern approach to Zurich airport through German airspace could be one notable example.

[106] Alison J. Williams, *supra* note 104: 52.

[107] Stuart Banner, *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On* (Cambridge (MA): Harvard University Press, 2008), p. 40-43.

International Civil Aviation in 1944.[108] More recently, the 1999 Montreal Convention had reaffirmed this trend. At first – and the crucial similarity to the modern perception of the cyberspace is striking – the air was envisaged as a new ocean, a new space of globally free movement and communication, unhindered by terrestrial borders and interests.[109] However, such visions have (been) never fulfilled. In addition, a significant degree of arbitrariness still remains in the very definition of the airspace, especially concerning the distinction between the air space, which is heavily regulated, and the outer space, which is free because this distinction is not natural but based on technology, and therefore potentially negotiable,[110] the current limit being at 100 kilometres, where the atmosphere is no longer suitable for conventional aircraft to fly.[111] Coming back to the cyberspace, such artificial boundaries could also be created or negotiated in there. Thus in the cases of the spaces without *external* limits – as opposed to the sea which has no natural *internal* limits but has the coastline as its *external* limit – be it the air or the cyberspace, it is the *capability to appropriate control* (i.e. technology) that determines what actually (or potentially) is regulated and what is not.

2.4. APPROPRIATION, TRADE, AND THE TRANSFORMATION OF THE PIRATE

As the sea had been transformed into a limitless trade and military transit route, so was the position of a pirate transformed from a noble adventurer into an outlaw or, according to Grotius, an enemy of whole humankind (*hostis humani generis*).[112] As a result, the pirate could not be encountered as an equal because of the pirate being positioned outside of the laws of war; hence he must be simply destroyed, and the war against pirates is always just.[113] As Michael Kempe notes, "[i]dentifying 'the other' as a sea brigand and murderer implies the latter's criminalisation as well as delegitimation as an equal combatant in war".[114] Such delegitimation was what Grotius had originally intended to apply for the Spanish and the Portuguese, but it also applies to pirates in general. For Grotius, who first

[108] Pablo Mendes De Leon, "The Dynamics of Sovereignty and Jurisdiction in International Aviation Law": 484-485; in: Gerard Kreijen, ed., *State, Sovereignty, and International Governance* (Oxford and New York: Oxford University Press, 2002).

[109] Stuart Banner, *supra* note 107, p. 53.

[110] Alexandra Harris and Ray Harris, "The Need for Air Space and Outer Space Demarcation," *Space Policy* 22 (2006): 4.

[111] Alison J. Williams, "Blurring Boundaries / Sharpening Borders: Analysing the US's Use of Military Aviation Technologies to Secure International Borders, 2001-2008": 288; in: Doris Wastl-Walter, ed., *The Ashgate Research Companion to Border Studies* (Farnham and Burlington: Ashgate, 2011).

[112] Carl Schmitt, *supra* note 73, p. 44.

[113] Michael Kempe, "Beyond the Law. The Image of Piracy in the Legal Writings of Hugo Grotius": 389; in: Hans W. Blom, ed., *Property, Piracy and Punishment: Hugo Grotius on War and Booty in De Iure Praedae – Concepts and Contexts* (Leiden: Brill, 2009).

[114] *Ibid*.: 385.

and foremost represented the interests of Dutch merchants, a pirate who posed as much danger to sea trade as an enemy vessel had to be completely outlawed,[115] just as the ships which belonged to Portugal or Spain, because these states, adhering to the image of the closed seas, were seen as attempting to hinder free maritime trade.[116] Today similarly to the sea pirates cybercriminals are challenging the global flows of finance and property. Cyber threats include copyright infringement (not surprisingly, the main push for legal sanctions against peer-to-peer (P2P) file-sharing sites, for example, the Piratebay, come from the copyright holders, i.e. multimedia, film, music, and software industry[117]), identity theft and denial of service (DoS) attacks, often committed for financial benefit.[118]

Although in mid-twentieth century maritime piracy was seen as a phenomenon of the past – and therefore was barely mentioned in most sea-related treaties and other documents regulating the high seas at that time[119] – currently the danger piracy poses is as acute as ever. Quite naturally, the states appear to pursue a situation-based and context-specific modus operandi as to tackling piracy when a specific problem arises – and not only regarding piracy but also when other maritime security threats such as smuggling weapons and drugs are concerned.[120] The relatively recent surge in pirate activity clearly illustrates that once the opportunity is ripe, for example, there is no strong local government capable and/or willing to tackle pirate activities, supply of offenders is vast because of widespread poverty combined with existing guerrilla movements or militias attempting to finance pirates' activities. Also, the opportunities to carry out pirate activities occur more than occasionally. Current situation in the Gulf of Aden and off the coast of Somalia is the most evident example of current sea piracy, although East Africa, the Nigerian coast and South China seas have been and still are dangerous, while the Malacca Straits have been a hotspot until recently.[121] Somalia's case also is a great illustration of the fact that that the perception of a sea pirate has remained relatively unchanged since Grotius. Actually, the UN Security Council's and other international efforts to counter piracy off Somalia have once again positioned a pirate as an enemy of the humankind. Especially recalling Security Council Resolution 1816[122] which had authorised the states to use 'all

[115] *Ibid*.: 385-386

[116] Walter Prescott Webb, *supra* note 80, p. 332.

[117] Tara Touloumis, "Buccaneers and Bucks from the Internet: Pirate Bay and the Entertainment Industry," *Seton Hall Journal of Sports & Entertainment Law* 19 (2009): 253, 256.

[118] Chenfeng Vincent Zhou, Christopher Leckie, and Shanika Karunasekera, "A Survey of Coordinated Attacks and Collaborative Intrusion Detection," *Computers & Security* 19 (2010): 126.

[119] Robin Geiß and Anna Petrig, *Piracy and Armed Robbery at Sea* (Oxford and New York: Oxford University Press, 2011), p. 40-42.

[120] *Ibid*., p. 54.

[121] Douglas Guilfoyle, *supra* note 30: 691.

[122] *The situation in Somalia*, United Nations Security Council, Resolution no. 1816, UN Docs. S/RES/1816 (2008).

necessary means' to fight against pirates off Somalia can be understood, keeping in mind UN Security Council's common vocabulary, as an authorisation to use military force[123] hence, pirates, albeit indirectly, have been effectively positioned as enemies of humankind under Chapter VII of the UN Charter:[124] the international community is authorised to tackle what is seen as part of the threat to international peace and security posed by the situation in Somalia.[125] This is quantitatively (but not necessarily qualitatively) different from that of e.g. the Malacca Straits, where, although counter-piracy efforts have been conducted mostly by the littoral states (with some help from outside forces, especially from India and several European states that had volunteered to assist), they were once again pushed forward by the global community at various levels.[126] And yet, such global response cannot be fully understood without noting that both the Gulf of Aden and the Malacca Straits are important shipping routes, crucial to global trade. This fact helps to explain why these two regions attract more global attention than others and why Somali pirates are (and the Malacca Straits pirates were), in a sense, enemies of whole humankind to a larger extent than others.

Notably, maritime piracy, being significantly less 'ethereal' than its counterpart in the cyberspace, is significantly easier to tackle, however, the phenomenon has never been completely destroyed. Under current international law, a state can seize any pirate vessel or a vessel held by pirates, and the courts of the country that had carried out the seizure have the jurisdiction to try the offenders.[127] Such actions are not only endorsed by customary international law but most probably would also be in line with the human rights treaties; this is at least suggested by the European Court of Human Rights, for example, in the *Medvedyev* case,[128] especially in circumstances when imminent danger to persons and/or property is present.[129] As a matter of fact, suppression of piracy is so entrenched in theory and practice of the law of the sea that it has been used as a model for regulating combat against other illegal activities.[130] However it would be difficult to transfer existing practices from the material world to cyberspace, e.g. the challenge is not only the ability to seize but also to determine what the vessel (the set of data used for malign activity) is, let alone to apply the nationality principle effectively. And the question of jurisdiction remains fundamentally open. Finally, following an

[123] Douglas Guilfoyle, *supra* note 30: 694-695.
[124] Tullio Treves, *supra* note 72: 400-401.
[125] Douglas Guilfoyle, *supra* note 30: 695.
[126] Nazery Khalid, "With a Little Help from My Friends: Maritime Capacity-building Measures in the Straits of Malacca," *Contemporary Southeast Asia* 31 (3) (2009): 428.
[127] Tullio Treves, *supra* note 72: 302.
[128] *Medvedyev and Others v France*, ECHR Grand Chamber, Application no. 3394/03 (March 29, 2010).
[129] Stefano Piedimonte Bodini, "Fighting Maritime Piracy under the European Convention on Human Rights," *The European Journal of International Law* 22 (3) (2011): 835-837.
[130] Natalie Klein, *supra* note 98, p. 306.

increasing trend in the battlefield and, especially, post-conflict situations, an important part in tackling maritime piracy is played by private contractors, aiding where a state's own military capabilities are inadequate.[131] This brings maritime piracy closer to that in the cyberspace where private cyber security firms are crucial in identifying and tackling the threats.

2.5. GENERAL CONSIDERATIONS ON REGULATING THE GLOBAL SPACES

The history of treatment of the sea also reflects the basic pathways that a regulation of any global space might take. First, there is a possibility of complete appropriation and division, i.e. absolute sovereignty of several states over the entire space as reflected by the *rayas* drawn by the Spanish and the Portuguese. Second, there also is a possibility of freedom to use and exploit the global space leading to a near-anomie, i.e. the crux of the Grotian doctrine, when no state is able to exert full control over a space (or when a dominant power benefits from such freedom, as Britain did). The third solution is a combination of both and is possible when both the means and the incentives to control the global space (or at least large segments of it) are present, but the competition for control and the stakes of failure to do so are high enough so as to foster a compromise and collective appropriation. The latter option appears to be more or less already in place concerning the regulation of the airspace and the most likely in the long term concerning the cyberspace.

The fundamental question at stake is also found in Grotius but possibly as old as any enquiry into human order: how do people come to acknowledge and follow a will, an order, a sovereignty?[132] Or, in this case, how could one push forward a more or less universally accepted form of regulation, and how (if at all) it could be enforced? Once again, the development of the law of the sea can be illustrative. Historically, several conditions have contributed to its development: first, the very existence of a common order and the possibility of prognostication has always been an inclusive interest of all states; second, as it could be expected, change was relatively smooth when vital strategic interests of at least some powers were not at stake; when they were, more often than not the inclusive interest of many has overcome the exclusive interest of some (as was the case with the Grotian theory itself),[133] but the powerful sovereign states have nevertheless been able to hinder

[131] Natalino Ronzitti, "The Use of Private Contractors in the Fight against Piracy: Policy Options": 38-39; in: Francesco Francioni and Natalino Ronzitti, eds., *War by Contract: Human Rights, Humanitarian Law, and Private Contractors* (Oxford and New York: Oxford University Press, 2011).
[132] Den Hartogh and Cees Maris, *supra* note 85: 107-108.
[133] David Armitage, *supra* note 78: 30.

the development of an inclusive international law.[134] As the current debate over the regulation of cyberspace illustrates, whereas an inclusive interest is clearly acknowledged, it is the second clause, i.e. the clash strategic interests of power-states that causes significant problems as far as the prospects of regulation are concerned.

As a general indication there are three reasons for a state/ the states to desire regulation of the cyberspace (or any other global space): sovereignty, security and economy. Sovereignty is a general term referring to a state's attempt to preserve its unique status and influence as well as its own particular standing in the global context. Although it is true that the modern world order poses many challenges to national sovereignty and the privileged status of states (cyberspace itself being one of the major contributors to this shift), the regulation of all global spaces is still subject to the power game among the most powerful states. In this power game two conflicting aims of actors can be outlined: 1) to preserve (and/or expand) one's influence; 2) to change the status quo into a more favourable one. The multi stake-holder approach, advocated by the US, is a clear illustration of the first aim, even if not a completely outright one.

Currently cyberspace is supervised by several non-profit bodies, based in the US and under significant influence from the US government, and partly regulated by markets, once again dominated by the US (leaving aside the fact that most of the content in cyberspace is generated in the US). This stands in stark contrast to international regulation, e.g. by the ITU, which has only indirect influence over the Internet; moreover, after the failure of the World Conference on International Telecommunications, a consensus on international governance seems even less likely.[135] Thus, although cyberspace is, in theory, free and self-regulating, in reality it often acts as an extension of the US 'soft power'. As a result, the US strongly reject any transfer of regulatory power to international agencies, including those within the UN system, presenting it as hampering competition and restricting the existing freedoms.[136] In this, the US act similarly as Britain did in upholding the Grotian doctrine of the free sea of which it was the master. There could be two counter-hegemonic strategies in this instance: one, if a state is strong enough, to pursue one's own hegemony; second, if a state is not as strong as to replace the current hegemon, to change the status quo into a less unfavourable one. The latter is the strategy employed by Russia, China and other developing countries: unable

[134] Natalie Klein, *supra* note 98, p. 326.

[135] "Internet Regulation: A Digital Cold War?" *The Economist* (December 14, 2012) // http://www.economist.com/blogs/babbage/2012/12/internet-regulation (accessed December 14, 2012).

[136] US Department of State, "Fast Facts on United States Submitting Initial Proposals to World Telecom Conference" (August 1, 2012) // http://www.state.gov/e/eb/rls/fs/2012/195921.htm (accessed November 4, 2012).

to assume the control of cyberspace themselves, they strive to at least curb the US influence by strengthening the regulation of cyberspace and urging the allocation of regulatory powers to international organisations, preferably to UN bodies, which is not surprising given the Russian and the Chinese influence in the UN. Such move is again presented as one towards a greater freedom because regulation by the UN would, in theory if not in practice, mean regulation by all states).[137] Therefore, the current situation in the cyberspace could be compared to the crisis of the regulation of the sea after the rise of new potent powers at the beginning of the 20th century.

As an additional crucial issue related to sovereignty, one could add that borders in general have multiple importance. They are not only the limits of sovereign power but also a matter of inclusion and exclusion, declaration of what does and what does not belong to the 'us' of a political community. They are also about classification and stratification, both external and internal. In addition, they create a common space, a sort of 'public sphere' by filtering its content. Therefore, they have to be constructed and managed.[138] As a result, the control of borders and the (material or immaterial) flows through them is also of vital importance to sovereignty.

Security is the second crucial issue. As more and more strategic functions of the state and corporate bodies, including those of control and command, are transferred to cyberspace, cyber warfare emerges as a new, more sophisticated form of conflict (similarly, the appropriation of the sea had once created naval warfare, and, much more recently, the appropriation of the air had created aerial warfare). As in the 'physical' world, states, privateers and brigands (including terrorists), with their different motivations, grievances, aims, and degrees of sophistication provide a wide spectrum of sources of threat that cannot be ignored.[139] Controlling (and often policing) cyberspace is, then, of strategic (and sometimes even vital) importance. Therefore, the aforementioned hegemonic struggle appears to be set not only to continue but to intensify even further.

Finally, the importance of economic aspects of cyberspace cannot be disregarded. Not only it has become an important space for flows of goods (and, quite possibly, of the most valuable goods of all), the place of almost inexhaustible riches, at least in theory available to all – almost analogous to the sea as imagined by Grotius. The ability to control these trade routes and the access to riches is at the core of a powerful state's economic interests. Furthermore, keeping in mind the

[137] "Russia Calls for Internet Revolution," *Russia Today* (May 28, 2012) // http://www.rt.com/news/itu-internet-revolution-russia-386 (accessed November 4, 2012).
[138] David Newman, "Contemporary Research Agenda in Border Studies: An Overview": 35; in: Doris Wastl-Walter, ed., *The Ashgate Research Companion to Border Studies* (Farnham and Burlington: Ashgate, 2011).
[139] Martin C. Libicki, *Cyberdeterrence and Cyberwar* (Santa Monica, Arlington, and Pittsburgh: The RAND Corporation, 2009), p. 4-5.

extremely high level of integration between governments and businesses, it comes as no surprise that the cyberspace regulation is very high on the agenda of international politics.

CONCLUSIONS

If a functioning cyberspace regulation framework is not established, there is an acute danger of a cyber 9/11 or cyber Pearl Harbor that would shake the entire status quo.[140] However, the challenges posed by cybercrime require a global response. Domestic laws and international agreements in the real word are ineffective in tacking the problems without working mechanisms in cyberspace itself. The means and techniques of catching pirates be it sea or cyberspace are different from those of apprehending criminals on land. Therefore, the understanding of law and law-enforcement needs to be transformed. For example, Lessig proposed the concept of four modalities of constraint – law, social norms, markets, and architecture – which could be used to effectively control cyberspace.[141] However, as once was the sea and air, cyberspace still remains rather unexplored and uncontrolled. Until effective control mechanisms are found and agreed upon, there will be 'pirates' who engage in criminal activity because of convenience to hide traces in the uncontrolled space. And still there is an ever present question of who can legitimately enforce the agreements and who can legitimately even start the negotiations for such agreements and decide what mechanisms and what laws are to regulate cyberspace at all.

In search for a solution, it is useful to draw an analogy with the other global spaces, most importantly, with the sea. There are several important similarities between the two that offer useful insights. Firstly, cyberspace, just like previously the sea, marks the border between the known and unknown, the controllable and the uncontrollable. This is true as far as both the popular imagination and the states' actual ability to exert their jurisdiction are concerned. Secondly, the cyberspace, again similarly to the sea, has become an immeasurable trade route and a space of abundant resources. Thirdly, it has also become an object of political and military struggle as states seek to both protect themselves and their economies and to transform this new space into an asset in their struggle for influence on a global scale. It is precisely the history of perception and regulation of the sea (and, to a lesser extent, of the air), that provides an insight into the power struggles and the importance of technological developments in setting the scene for possible

[140] Charles J. Dunlap, "Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors," *Nebraska Law Review*, 87 (2008-2009): 723.

[141] Lawrence Lessig, "The Law of the Horse: What Cyberlaw Might Teach," *Harvard Law Review* 113 (1999): 501-546.

regulatory frameworks. It can be deduced from the history of the regulation of the sea that the states will continuously strive to slice off as much control over cyberspace as is technologically possible, thus aiming to ensure their vital interests as well as to undermine those of others. As it has been shown, even a doctrine of the free sea can be upheld by a hegemonic power (Britain and the US respectively) first and foremost with a view to prevent competition. The same currently applies to cyberspace. However, despite a continuing dominance by the US, the current situation in cyberspace appears to more resemble that in the sea at the beginning of the 20th century, where the rise of a number of potent powers pushed the old system to disarray and led to the modern mixture of freedom and appropriation. As a result, envisaging the cyberspace as regulated by a treaty similar to the United Nations Convention on the Law of the Sea (UNCLOS) would be a viable exercise.

Finally, the treatment of cybercrime – piracy in the new sea of cyberspace – is also closely related to what the states, the businesses, and other actors make of the new global space. Just as pirates have been outlawed and turned into enemies of humanity when the high seas were appropriated for commercial purposes, cybercrime became an acute global danger when the cyberspace was transformed into a medium of communication and trade. It is no longer am often romanticised hacker cracking codes in a dimly-lit room but an international criminal, often associated with cartels and syndicates but also increasingly backed by sovereign states in their endeavours against other states. The latter is not a new phenomenon but one already successfully employed in the seas by the British, the French, or the Dutch in their struggle against the Spanish and the Portuguese dominance of the New World.[142] And yet, despite occasional secret backing, the governments are under intense pressure from businesses and other stakeholders to tackle cybercrime effectively.

All things considered, increased regulation of the internet appears to be unavoidable. The issue that remains, however, is central: how to achieve an agreement between the states and other core actors of the cyberspace. And it is here that one could and should take important lectures from history.

BIBLIOGRAPHY

1. Armitage, David. "The Elephant and the Whale: Empires of Land and Sea." *Journal for Maritime Research* 9 (1) (2007): 23-36.
2. Banner, Stuart. *Who Owns the Sky? The Struggle to Control Airspace from the Wright Brothers On.* Cambridge (MA): Harvard University Press, 2008.

[142] Douglas R. Burgess, *supra* note 3: 302-303.

3. Blau, John. "Battle Brewing over International Internet Regulation." *IEEE Spectrum* (December 2012) // http://spectrum.ieee.org/telecom/internet/battle-brewing-over-international-internet-regulation (accessed December 14, 2012).
4. Bodini, Stefano Piedimonte. "Fighting Maritime Piracy under the European Convention on Human Rights." *The European Journal of International Law* 22 (3) (2011): 829-848.
5. Brenner, Susan W., and Marc D. Goodman. "The Emerging Consensus on Criminal Conduct in Cyberspace." *International Journal of Law and Information Technology* 10 (2) (2002): 139-223.
6. Burgess, Douglas R. "Hostis Humani Generi: Piracy, Terrorism and a New International Law." *University of Miami International and Comparative Law Review* 13 (2006): 293-341.
7. Cade, Nicholas W. "An Adaptive Approach for an Evolving Crime: The Case for an International Cyber Court and Penal Code." *Brooklyn Journal of International Law* 37 (3) (2012): 1139-1175.
8. Caral, Jose MA. Emmanuel. "Lessons from ICANN: Is the Self-regulation of the Internet Fundamentally Flawed?" *International Journal of Law and Information Technology* 12 (1) (2004): 1-31.
9. Cerf, Vinton, Barry M. Leiner, David C. Clark, *et al*. "A Brief History of the Internet", *An International Electronic Publication of the Internet Society* (1997) // http://www.isoc.org/oti/printversions/0797prleiner.html (accessed December 17, 2012).
10. Chik, Warren B. "'Customary Internet-tional Law': Creating a Body of Customary Law to Cyberspace. Part 1: Developing Rules for Transitioning Custom into Law." *Computer Law & Security Review* 26 (2010): 3-44.
11. Clough, Jonathan. "Cybercrime." *Commonwealth Law Bulletin* 37 (4) (2011): 671-680.
12. Clough, Jonathan. "Data Theft? Cybercrime and the Increasing Criminalization of Access to Data." *Criminal Law Forum* 22 (1) (2011): 145-170.
13. Connery, Christopher L. "Ideologies of Land and Sea: Alfred Thayer Mahan, Carl Schmitt, and the Shaping of Global Myth." *Elements* 28 (2) (2001): 173-201.
14. De Leon, Pablo Mendes. "The Dynamics of Sovereignty and jurisdiction in International Aviation Law": 483-496. In: Gerard Kreijen, ed. *State, Sovereignty, and International Governance*. Oxford and New York: Oxford University Press, 2002.

15. Dean, Mitchell. "Nomos: Word and Myth": 242-258. In: Louiza Odysseos and Fabio Petito, eds. *The International Political Thought of Carl Schmitt: Terror, Liberal War, and the Crisis of Global Order.* Abingdon and New York: Routledge, 2007.

16. Dunlap, Charles J. "Towards a Cyberspace Legal Regime in the Twenty-First Century: Considerations for American Cyber-Warriors." *Nebraska Law Review* 87 (2008-2009): 712-724.

17. Frazzetto, Mark. "A Maritime Model for Cyberspace Legal Governance." *The National Strategy Forum Review* (September 19, 2011) // http://nationalstrategy.wordpress.com/ (accessed November 4, 2012).

18. Geiß, Robin, and Anna Petrig. *Piracy and Armed Robbery at Sea.* Oxford and New York: Oxford University Press, 2011.

19. Ghosh, Sumit, and Elliot Turrini. *Cybercrimes: A Multidisciplinary Analysis.* Heidelberg: Springer, 2010.

20. Grabosky, Peter. "The Global Dimension of Cybercrime." *Global Crime* 6 (1) 2004: 146-157.

21. Greenleaf, Graham. "Regulating Cyberspace: Architecture vs Law?" *University of New South Wales Law Journal* 21 (2) (1998): 593-604.

22. Grewe, Wilhelm G. *The Epochs of International Law.* Berlin: Walter de Gruyter, 2000.

23. Guilfoyle, Douglas. "Piracy off Somalia: UN Security Council Resolution 1816 and IMO Regional Counter-Piracy Efforts." *International Criminal Law Quarterly* 57 (2) (2008): 690-699.

24. Harris, Alexandra and Ray Harris. "The Need for Air Space and Outer Space Demarcation." *Space Policy* 22 (2006): 3-7.

25. Hartogh, Den, and Cees Maris. "The Commencement of Modern Age": 91-110. In: Cees Maris and Frans Jacobs, eds. *Law, Order and Freedom: A Historical Introduction to Legal Philosophy.* Heidelberg; Springer, 2011.

26. Illves, Toomas Hendrik. "It's the Economy, Stupid!" *The Security Times* (September 2012): 24.

27. "Internet Regulation: A Digital Cold War?" *The Economist* (December 14, 2012) // http://www.economist.com/blogs/babbage/2012/12/internet-regulation (accessed December 14, 2012).

28. Jarvie, Natasha. "Control of Cybercrime – Is an End to Our Privacy on the Internet a Price Worth Paying? Part 1." *Computer and Telecommunications Law Review* 9 (3) (2003): 76-81.

29. Jarvie, Natasha. "Control of Cybercrime – Is an End to Our Privacy on the Internet a Price Worth Paying? Part 2." *Computer and Telecommunications Law Review* 9 (4) (2003): 110-115.

30. Johnson, David and David Post. "Law and Borders – The Rise of Law in Cyberspace." *Stanford Law Review* 48 (1996): 1367-1402.

31. Joint Chiefs of Staff, Department of Defense Dictionary of Military and Associated Terms. "Joint Publication 1-02" (2001) // http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed November 4, 2012).

32. Judy, Henry L., and David Satola. "Business Interests Under Attack in Cyberspace: Is International Regulation the Right Response?" *Business Law Today* (December 2011) // http://apps.americanbar.org/buslaw/blt/content/2011/12/article-2-judy-satola.shtml (accessed November 4, 2012).

33. Kadens, Emily. "The Myth of the Customary Law Merchant." *Texas Law Review* 90 (5) (2012): 1153-1206.

34. Kempe, Michael. "Beyond the Law. The Image of Piracy in the Legal Writings of Hugo Grotius": 379-395. In: Hans W Blom, ed. *Property, Piracy and Punishment: Hugo Grotius on War and Booty in De Iure Praedae – Concepts and Contexts.* Leiden: Brill, 2009.

35. Khalid, Nazery. "With a Little Help from My Friends: Maritime Capacity-building Measures in the Straits of Malacca." *Contemporary Southeast Asia* 31 (3) (2009): 424-446.

36. Klein, Natalie. *Maritime Security and the Law of the Sea.* Oxford and New York: Oxford University Press, 2011.

37. Kleinwachter, Wolfgang. "Internet Governance Outlook 2012: Cold War or Constructive Dialogue." *Communications Law* 17 (1) (2012): 14-18.

38. Klimburg, Alexander. "Mobilising Cyber Power." *Survival: Global politics and Strategy* 53 (1) (2011): 41-60.

39. Koops, Bert-Jaap. "The Internet and its Opportunities for Cybercrime": 735-754. In: M Herzog-Evans, ed. *Transnational Criminology Manual*. Nijmegen: Wold Legal Publishers, 2010.

40. Lessig, Lawrence. "The Law of the Horse: What Cyberlaw Might Teach." *Harvard Law Review* 113 (1999): 501-546.

41. Libicki, Martin C. *Cyberdeterrence and Cyberwar.* Santa Monica, Arlington, and Pittsburgh: The RAND Corporation, 2009.

42. Maier, Bernhard. "How Has the Law Attempted to Tackle the Borderless Nature of the Internet?" *International Journal of Law and Information Technology* 18 (2) (2010): 142-175.

43. Marder, Michael. *Groundless Existence: The Political Ontology of Carl Schmitt.* New York and London: Continuum, 2010.

44. Mayer, Franz C. "The Internet and Public International Law – Worlds Apart?" *European Journal of International Law* 12 (3) (2001): 612-622.

45. Menthe, Darrel C. "Jurisdiction In Cyberspace: A Theory of International Spaces." *Michigan Telecommunications Law Review* 4 (1998): 69-103.

46. Newman, David. "Contemporary Research Agenda in Border Studies: An Overview": 33-48. In: Doris Wastl-Walter, ed. *The Ashgate Research Companion to Border Studies.* Farnham and Burlington: Ashgate, 2011.

47. O'Donnovan, Oliver, and Joan Lockwood O'Donnovan. "Isidore of Seville": 204-206. In: Oliver O'Donnovan and Joan Lockwood O'Donnovan, eds. *From Irenaeus to Grotius: A Sourcebook in Christian Political Thought, 100-1625*. Grand Rapids and Michigan: William B. Eerdmans Publishing, 1999.

48. Odysseos, Louiza, and Fabio Petito. "The International Political Thought of Carl Schmitt": 1-18. In: Louiza Odysseos and Fabio Petito, eds. *The International Political Thought of Carl Schmitt: Terror, Liberal War, and the Crisis of Global Order.* Abingdon and New York: Routledge, 2007.

49. Orji, Uchenna Jerome. "An Analysis of China's Regulatory Response to Cybersecurity." *Computer and Telecommunications Law Review* 18 (7) (2012): 212-226.

50. Pardo, Arvid. "The Law of the Sea: Its Past and its Future." *Oregon Law Review* 63 (1) (1984): 7-17.

51. Reed, Chris. "Online and Offline Equivalence: Aspiration and Achievement." *International Journal of Law and Information Technology* 18 (3) (2010): 248-273.

52. Ronzitti, Natalino. "The Use of Private Contractors in the Fight against Piracy: Policy Options": 37-53. In: Francesco Francioni and Natalino Ronzitti, eds. *War by Contract: Human Rights, Humanitarian Law, and Private Contractors.* Oxford and New York: Oxford University Press, 2011.

53. "Russia Calls for Internet Revolution." *Russia Today* (May 28, 2012) // http://www.rt.com/news/itu-internet-revolution-russia-386 (accessed November 4, 2012).

54. Schmitt, Carl. *The Nomos of the Earth in the International Law of Jus Publicum Europaeum.* New York: Telos, 2003.

55. Scott, Jennifer. "ITU Internet Regulation Blocked by UK and US." *ComputerWeekly.com* (December 14, 2012) // http://www.computerweekly.com/news/2240174668/ITU-regulation-blocked-by-UK-and-US (accessed December 14, 2012).

56. Stahl, William M. "The Uncharted Waters of the Cyberspace: Applying the Principles of International Maritime Law to the Problem of Cybersecurity." *Georgia Journal of International and Comparative Law* 40 (2011): 247-273.

57. Touloumis, Tara. "Buccaneers and Bucks from the Internet: Pirate Bay and the Entertainment Industry." *Seton Hall Journal of Sports & Entertainment Law* 19 (2009): 253-281.

58. Treves, Tullio. "Piracy, Law of the Sea, and Use of Force: Developments off the Coast of Somalia." *European Journal of International Law* 20 (2) (2009): 399-414.

59. US Department of State. "Fast Facts on United States Submitting Initial Proposals to World Telecom Conference" (August 1, 2012) // http://www.state.gov/e/eb/rls/fs/2012/195921.htm (accessed November 4, 2012).

60. Wang, James C. F. *Handbook on Ocean Politics and Law.* Westport: Greenwood Press, 1992.

61. Webb, Walter Prescott. *The Great Frontier.* Reno: University of Nevada Press, 2003.

62. Williams, Alison J. "A Crisis in Aerial Sovereignty? Considering the Implications of Recent Military Violations of National Airspace." *Area* 42 (1) (2010): 51-59.

63. Williams, Alison J. "Blurring Boundaries / Sharpening Borders: Analysing the US's Use of Military Aviation Technologies to Secure International Borders, 2001-2008": 283-300. In: Doris Wastl-Walter, ed. *The Ashgate Research Companion to Border Studies.* Farnham and Burlington: Ashgate, 2011.

64. Yar, Majid. "The Novelty of 'Cybercrime': An Assessment in Light of Routine Activity Theory." *European Journal of Criminology* 2 (2005): 407-427.

65. Zekos, Georgios I. "Globalisation and States' Cyber- Territory." *Web Journal of Current Legal Issues* 5 (2001) [pagination not available].

66. Zhou, Chenfeng Vincent, Christopher Leckie, and Shanika Karunasekera. "A Survey of Coordinated Attacks and Collaborative Intrusion Detection." *Computers & Security* 19 (2010): 124-140.

LEGAL REFERENCES

1. *Anglo-Norwegian Fisheries Case*. I.C.J. Reports 1951, 116.
2. *Convention on Cybercrime*. Council of Europe. CETS no. 185 (Budapest; November 23, 2001).
3. *eDate Advertising GmbH v X (C-509/09) and Olivier Martinez and Robert Martinez v MGN Limited (C-161/10)*. European Court of Justice. Opinion of Advocate General Cruz Villalon (March 29, 2011).
4. *League against Racism and Antisemitism (LICRA), French Union of Jewish Students v Yahoo! Inc. (USA), Yahoo France*. Tribunal de Grande Instance de Paris (The County Court of Paris). Interim Court Order (November 20, 2000). Electronic Business Law Reports 1(3) (2001): 110-120.
5. *Medvedyev and Others v France*. ECHR Grand Chamber. Application no. 3394/03 (March 29, 2010).
6. *The Situation in Somalia*. United Nations Security Council. Resolution no. 1816. UN Docs. S/RES/1816 (2008).
7. *Towards a General Policy on the Fight against Cyber Crime*. The Council and the Committee of the Regions. Communication from the Commission to the European Parliament. COM/2007/0267 Final. {SEC(2007) 641} {SEC(2007) 642}.