TILBURG LAW SCHOOL

-LLM Law & Technology-

International Regulation of National Cybercrime Jurisdiction

Önder Kutay Şeker
ANR: 917331

Paul J.A. de Hert
Thesis Supervisor

CONTENTS

Introduction

The thesis is divided into five chapters; each answering to a different aspect of the multi-faceted main question and building up towards a comprehensive answer at the end. Since every thesis is an attempt to answer a major question, the first chapter, ***"How Did Cybercrime Jurisdiction Turn Into A Major Problem?"***, aims to explain two very basic but essential questions that every reader should ask themselves before reading this thesis: 1-Why there is a problem regarding the international jurisdiction of cybercrime? 2-Why there is no simple solution to that problem? Therefore, the first chapter is fundamentally supplying the necessary background information to illustrate the concerns that gave birth to the main question.

Then in the second chapter, named ***"Conventional Jurisdictional Approaches and Cybercrime"***, first the concept of jurisdiction is explained in detail; starting from its historical definitions and advancing towards its newfound limits. After that, interactions between various international law principles, on which jurisdictional claims are established, and certain types of cybercrime are analyzed. The main question this chapter answers is: "How does various approaches to jurisdiction interact with cybercrime in the current state of the world?" While doing this, laws and court decisions from three selected countries have been used mainly. These countries are: United States of America, United Kingdom and Germany. This choice can only be considered partially arbitrary, for our criteria were the following: 1- "Highly wired"[1] or "Internet dependent" countries should be selected for the purposes of any kind of cybercrime analysis; since these countries are pioneering cyber law along with the technological advancement 2-

[1] Highly wired countries are those heavily reliant upon networks and systems to support vital systems such as transportation, power grid, water distribution, health and so on and also with a high percentage of their population connected to the Internet.

Countries with established legal tradition and case-law regarding cybercrime are preferable in order to conduct an accurate legal research since they provide more data to examine 3- Countries with relatively high political power are preferable since international law is more likely to be shaped by the practices of these countries. 4- The last criterion was to choose countries with different approaches in order to reflect the diversity of opinions. Therefore our first choice was the United States of America which fulfilled the first three criteria to a great extent and which had a strikingly different approach towards content crimes than the rest of the world due to the 1st Amendment[2]. The United Kingdom, while having a similar legal system to USA, surprisingly had a substantially different approach towards the subject even upon the first examination. Since the UK also satisfied the first three criteria we were inclined to include them. Germany, on the other hand, not only had a completely contradicting view with the first two countries on certain topics but also it was necessary to represent a continental European approach. Nevertheless, several other countries' laws have also been referred in multiple instances throughout the thesis.

The following chapter, ***"Conflicts of Jurisdiction and the Dispute of Priority"*** is indeed a follow-up to the second chapter. Besides the principals that serve as a ground to establish jurisdiction, there are some principals that can limit the ability of a state to prescribe its domestic laws and/or give priority to a state's claim above others. Here we first tried to explain how conflicting claims of jurisdiction -or in some cases lack of any jurisdiction claims- occur in the current international system. Then we analyzed the national laws and court decisions of our sample countries along with some principles of international public law regarding conflicts of

[2] 1st Amendment to the Bill of Rights, (1791) *"Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech or of the press…"*

jurisdiction to answer the question: “To what extent jurisdictional problems raised by cybercrime can be addressed with these rules?”

In the fourth chapter this time two international agreements that are highly relevant to international jurisdiction of cybercrime and international cooperation are analyzed. The aim of this chapter is to show the road so far in the international arena and is named as ***“Convention on Cybercrime, ACTA and the Future of Cybercrime Jurisdiction”***.

Shortly after the supranational attribute of cybercrime was widely recognized, the idea of an international agreement that can regulate cybercrime jurisdiction emerged in order to overcome conflicting provisions in national laws and enhance international cooperation. Convention of Cybercrime and ACTA are the products of this approach. However the tendencies in these agreements made us question the allegedly positive role of international cooperation for jurisdiction in cyberspace. Thus the main question attempted to be answered in this last chapter is: “How international cooperation shapes international jurisdiction and what will be the future of cybercrime jurisdiction, given that current trends continue?”

Finally in the ***Conclusion***, we summarized our findings and tried to engineer possible solutions to the problems of cybercrime jurisdiction and also shared our general observations on the changing nature of jurisdiction and sovereignty itself.

Chapter 1: How did Cybercrime Jurisdiction turn into a major problem?

0. Intro

The rate of transformation -or evolution so to say- in cybercrime is perhaps outmatching any predecessor in the field of Criminal Law and the responses of even the most developed jurisprudences in this specific field has been rather slow according to a vast majority of scholars. However jurisdictional problems in a specific field of criminal law are even slower to emerge as they appear as a collateral effect of a change in the text or interpretation of a criminal code.

In the first section of this chapter, we attempted to summarize the current state of cybercrime activities in order to provide a better perspective of what we are aiming to regulate. This emphasis was actually necessary in order to clarify why cybercrime is dissimilar to other types of criminal acts; especially since these properties do matter in conjunction with jurisdiction clauses. Then in the second section, which is essentially a short introduction to the concept of international jurisdiction, we pointed out this interaction between the distinctive properties of cybercrime and the functioning of international jurisdiction.

In the third section, we wanted to demonstrate the legal oddities that can occur when the current system of international jurisdiction rules is applied to cybercrimes by the help of some infamous cases. Finally in the fourth section, we tried to set the ground rules for any potential idea that aims to improve the current system.

1. Distinctive Qualities of Cybercrime

The current attributes of cybercrime, in essence, is reliant on the change of mentality among cybercriminals within the last decade; that now, cybercrime is more of an instrument of

financial gain than its earlier examples.[3] This new criminal approach consequently caused a shift in behavioural patterns of cybercriminals; that they assumed subtlety instead of seeking acknowledgement and reputation for their feats.[4] Not only had the cybercriminals become stealthier but their array of techniques for hacking and infiltrating has also profoundly improved. This consequently changes the victim profile; that *"attacks are becoming increasingly personalized as information about occupation, gender, age and area of residence is sorted, using analytical software to profile individuals into potential victim groups."*[5] As it can be seen, cybercrime is more systematic and organized than before and some scholars even expect the emergence of cybercrime syndicates similar to drug cartels[6]; which would further enhance the capabilities of cybercriminals and the amount of threat they pose for the society; but at this point cybercrime already is fairly problematic.

The Internet and intranets all around the world are connecting everything; machine and human, with each other and therefore the range of cybercriminals is easily reaching beyond national borders. Almost all computer systems, including the most vital ones, are somehow connected to a network at least; therefore they are all potential victims of cybercrime and unfortunately most of these systems have little defence indeed when put to test against skilled and dedicated cyber warriors. Since 2006, USA Department of Homeland Security has been launching a cyber-war exercise called 'Cyber Storm'. The scenarios so far included some of the cataclysmic possible outcomes of a full-scale cyber assault against the nation such as; air control

[3] Wall, David S., 'Crime and Deviance in Cyberspace', 2009, *Introduction xvi*.

[4] Id.

[5] Id.

[6] *See:* Brenner, Susan W.; 'Organized Cybercrime? How Cyberspace May Affect the Structure of Criminal Relationships'

towers being shut down, water utilities being compromised, power grids[7] being assaulted and so on.[8] It is important to point out that, the threat cybercrime poses is real; however unlike the public expectation generated by such war-games and fiction, its effects are not greatly dramatic or flashy but rather invisible most of the time. It is indeed quite normal to be the target of a cybercrime and not even realize; as cybercrimes are not always evident or they might serve as preparatory acts to make more serious offenses possible.[9] Nevertheless the importance of such cyber exercises is that they reveal the magnitude of vulnerability against threats coming from the cyberspace.

The invisibility of cybercrimes absolutely does not mean that they lack consequences. The concern regarding cybercrimes is based on several elements; "*the most important being the problems law enforcement officials and prosecutors encounter in trying to apply existing law to cyberspace crime.*"[10] There has been some progress in the field of criminalizing and categorizing cybercrime within the last decade; however enforcing these laws still create problems due to three main problems: 1- Cybercrime rapidly morphs into new and different forms[11] 2- Cybercrime tends to fall outside the experience of the criminal justice systems[12] 3- Cybercrime is

[7] In April 2007, in Idaho, USA, a governmental lab actually tested if a cyber-warrior can remotely destroy an electric generator; in an experiment code-named 'Aurora' and they confirmed that it is actually quite possible.
Clarke, Richard A.; Knake, Robert K.; 'Cyber War', 2010, p.100

[8] USA Department of Homeland Security; http://www.dhs.gov/files/training/gc_1204738275985.shtm [Last Visited: 30.06.2012]

[9] Wall, David S., *Introduction xix.*

[10] Goodman, Marc D.; Brenner, Susan W.; 'The Emerging Consensus on Criminal Conduct in Cyberspace', 2002, p.1

[11] Id. p.3

[12] Wall, David S., *Introduction xx.*

global/transnational and assuming a national focus only is not sufficient enough to combat against it.[13]

2. The Enhanced Importance of International Jurisdiction Regime

Among these issues especially the third one is the main focus of this thesis; because in the current situation resolving both negative and positive jurisdictional conflicts regarding cybercrime is challenging. Even when there is no jurisdictional conflict another problem emerges: *"countries…have to consider searching for digital evidence themselves…through computer networks, and start prosecutions in their own country against foreign cybercriminals"*.[14] However doing so may also raise conflicts over sovereignty and jurisdiction;[15] since states, by default, are considered to have jurisdiction over crimes that are committed inside their territorial boundaries and exceptions to this principle are strictly defined.[16] As a result, the international community has been trying to improve international cooperation for prosecuting cybercrime through bilateral and multilateral agreements; since the current system is more or less reliant on cooperation. Nevertheless it is safe to say here that, a reliable system for cybercrime prosecution should not be mainly dependent on cooperation; as it is not always guaranteed and simply because without the capability of cross-border enforcement, prosecuting transboundary cybercrimes is futile.[17] This leads us to an important question: "to what extent a country can claim extraterritorial jurisdiction?" On the other hand, deciding on the location of cybercrimes is a rather challenging feat. As it will be demonstrated, states consider

[13] Koops, Bert-Jaap; Brenner, Susan W.; 'Cybercrime and Jurisdiction', 2006, p.1

[14] Id. p.2

[15] Id.

[16] *See*: **Chapter** 2, **Section** 5

[17] Koops & Brenner; 'Cybercrime and Jurisdiction', p.2

several crimes to have happened inside their territory while some parts of the crime actually transpired elsewhere.[18] Therefore we must reformulate the question as follows: "What should be the limit to jurisdiction claims in the case of cybercrimes that are partially or wholly committed on the territory of other states?"

3. An Overview of Current Problems in Cybercrime Jurisdiction

This legal discordance, led states to develop their own course of action. Some countries pursued rather unorthodox methods of prosecution and enforcement to overcome jurisdiction barriers when encountered by cybercrimes committed beyond their borders. In the very famous case of Alexey Ivanov and Vasiliy Gorshkov, the two Russian hackers who had been allegedly extorting money from several U.S. companies, the FBI used a ground-breaking methodology. In November 2000, the federal agents, hiding their true identity under the guise of businessmen, enticed the two Russian hackers to come to Seattle by offering them a job interview for positions in a network security company. The agents then asked the Russian duo to demonstrate their skills on computers readily infected by spyware and eventually 'hacked' the passwords Ivanov and Gorshkov used to access their own computers. Later the agents got into the computers of hackers, which were located in Russia and copied their contents to preserve evidence and pressed charges based on this evidence.[19] Furthermore, the U.S. Court that found Ivanov and Gorshkov guilty claimed that Russian law was not violated.[20] Consequently, Russian authorities and many others claimed that the evidence was obtained illegally and more importantly they claimed that

[18] *See* **Chapter** 2, **Section** 2 and 3

[19] Brenner, Susan W.; Koops, Bert-Jaap; 'Approaches to Cybercrime Jurisdiction', Journal of High Technology Law 2004, p. 21-22

[20] Koops & Brenner; 'Cybercrime and Jurisdiction', p. 322

the act was in violation of traditional jurisdictional boundaries.[21] Moreover, Russian authorities expressed their opposition to such usage of jurisdictive power by filing charges, against the FBI agents for hacking in Russia[22]; which actually is another jurisdictional question in itself. Even though this action may be deemed as symbolical; it is not. Recalling that state practice is a source of international law[23], dissent is a very important tool in preventing unapproved practices of other states from turning into customary international rules.

Beyond the international law related problems created by such an approach, it also has implications on individuals; that if such approach is commonly adopted, then *"citizens abiding by the laws of their country can find themselves subject to prosecution in another country under its different laws"*.[24] In the example of Ivanov and Gorshkov, the crime in question is hacking or in other words an unauthorized access to a computer system and altering data therein, which is a crime recognized under both American and Russian law. However there is no global consensus on what actions taking place within the Cyberspace shall be criminalized and it is hard to imagine what would have happened if the alleged act was only defined as a crime under United States laws.

On the other hand, when conventional jurisdiction theories and principles are fully applied to cybercrimes, either of the two is likely to happen in the case of a transboundary cybercrime: 1- the state(s) that can and should claim jurisdiction may not exercise its power 2- a state that should not have asserted jurisdiction may do so based on a fictitious link and start prosecution.

---

[21] Id. p. 323

[22] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p. 22

[23] The Statue of International Court of Justice, June 26, 1945, art. 38, 59 Stat. 1055, 1060.

The former may be caused by the lack of resources, legislation or if nothing else by lack of will to prosecute;[25] mostly resulting in cybercrimes going unpunished and encouraging cybercriminals to continue their ill deeds. For instance, in several nations of Africa and the Caribbean, cybercrime have not yet been criminalized at all and some countries that have criminalized cybercrimes lack the technical capability of tracking down suspects or gathering evidence.[26] Another possibility is that, even when more than one country can claim jurisdiction, none may do so; *"thinking that surely other countries will have suffered more damage and hence will have priority in prosecuting"*.[27] The latter appears to be a consequence of using inadequate jurisdictional laws and theories and causes the accused to be trialled in the wrong country, under wrong laws; which again defies the fundamental principles of criminal law and criminal procedure law and transgresses real and legal persons rights alike. A notable example of this is the incident of CompuServe[28]; in which German prosecutors charged Felix Somm, the executive manager of CompuServe Corp.'s Germany operations, whose company was accused as an accessory of dissemination of child pornography and extremist materials. Prosecutors claimed that his company should have blocked access to the objectionable material. Actually, the content was within discussion threads and was added by users which are not necessarily associated with CompuServe and moreover CompuServe did not carry discussion threads in their servers. Munich Administrative Court that trialled Somm decided in 1998 and found him guilty and gave

---

[24] Goodman & Brenner; p.54

[25] Koops & Brenner; 'Jurisdiction and Cybercrime', p.2

[26] Goodman & Brenner; p.83

[27] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.3

[28] CompuServe Corp. is a company based in Columbus, Ohio in USA and an Internet Service Provider. It was the first major commercial online service in the United States of America. The company currently operates as a subsidiary of AOL.

him a two-year suspended sentence. Somm appealed to this decision and a year later, the conviction was overturned and he was acquitted.[29] CompuServe is an American company and it could be trialled in front of a German court in account for its services. Obviously, the implications of this kind of practice are dire, as it puts ISPs and other actors of Internet - including users- under the threat of litigation in basically any country on the globe for their actions.

As epitomized by these two infamous incidents, the knife has two edges; while abiding by the traditional jurisdictional boundaries, states sometimes will not be able to effectively prosecute cybercrimes or in some cases they may prosecute crimes that they should not; and yet when they do not abide by such principles, their international relations will most likely be inversely affected and they will risk perpetrating international law. Additionally in both cases there is a substantial probability of violating the rights of the suspects/defendants.

4. Establishing the Ground Rules for a Possible Solution

The reason behind the above mentioned jurisdictional uncertainty has several reasons; but most of the time they are related to the regulations themselves. This is a flaw, a *bug* so to say, that occurs when legal principles that are meant to govern the field of "terrestrial" crimes are used in conjunction with cybercrimes. Susan W. Brenner stated the importance of this distinction ten years ago: *"While the world has slowly begun to deal with traditional border crossings, the nature of cyberspace is highly inconsistent with terrestrial based jurisprudence."*[30] And some six years before that David R. Johnson and David G. Post suggested *"conceiving Cyberspace as a*

[29] *See: PC World News, 17 April 1997,* http://www.pcworld.com/article/4591/compuserve_general_manager_faces_pornography_charge_in_germany.html (last visited: 30.06.2012)

distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the real world";[31] an idea not to be taken lightly, which will be further discussed while trying to reach a solution regarding today's jurisdictional issues. Therefore the similarities and differences of "terrestrial crimes" and "cybercrimes" have to be clarified and an analysis of the existing jurisdictional principles has to be done to decide which of them –if any- are applicable for cybercrime.

Legal problems, most of the time, are ignored when the consequences are minor and solitary, as in the examples given above but only taken serious when they cause massive and widespread harms. David Wall emphasizes this fallacy by these words: *"The routine experience of cybercrime to date is that it is individually invidious, but collectively insidious."*[32] A properly functioning jurisdictional system can and will help taking cybercrime under control before it becomes further organized and takes root into our societal mechanics. P.O. Träskman wrote: *"The intention, after all, is to develop international criminal law in a dynamic direction, towards a rational system where the jurisdictional competence of states is in fact limited to offences that cannot be punished as appropriately by another state."*[33] In fact coordination and reason might have solved the problem; but it is not the case in our current state of affairs; that we do not have the conditions of *civitas maxima*.[34] In our world, states tend to not to pay attention toward neither

---

[30] Id.

[31] Johnson, David R.; Post, David G.; 'Law and Borders – The Rise of Law in Cyberspace', Stanford Law Review 1996, Vol:48, p.1378

[32] Wall, David S.; *Introduction xx.*

[33] Wolswijk, H.D.; 'Locus Delicti and Criminal Jurisdiction', Netherlands International Law Review 1999, XLVI; p.381.

[34] Id.

the best benefits of other states or individuals that are not their citizens. Hostilities are widespread and villains sought by an unfriendly state are ignored or even sometimes protected.

Last but not least, the recent emergence of international legislations such as ACTA reveals that most states are willing to declare a 'cyber-curfew' and tyrannize the entire cyberspace by putting it under total surveillance in order to solve the fundamentally jurisdictional problems that are crippling the combat against cybercrime. It is indeed easier to maintain cyber security when individuals and companies are under constant threat of legal action against them; however using the threat of cybercrime as a pretext to severely restrain freedoms should not be the way to achieve success in this endeavour.

All in all, any solution that is to be provided for this predicament shall eliminate the possibility of cybercrime going unpunished; while keeping sovereignty of states intact as much as possible and shall have minimum or no impact on individual rights and freedoms. Acknowledging this, the purpose of this thesis is to seek the answer to following questions: Can international cooperation be regulated? If yes, what should be the nature of such regulated cooperation? If not, how can we tackle with this imminent problem?

Chapter 2: Conventional Jurisdictional Approaches and Cybercrime

0. Intro

As jurisdiction is the central term in this thesis, we dedicated the first chapter to the in-depth analysis of conventional definitions and applications of jurisdiction, types of jurisdiction and how these approaches interact with cybercrime.

Under the first section, we briefly introduced the historical roots of jurisdiction, types of jurisdiction, generally accepted grounds for asserting jurisdiction and the significant alterations in these over the course of time.

Legitimate grounds or theories for asserting jurisdiction is a topic of vital importance for this thesis and therefore in the second and third sections we went deeper in to subject by explaining the first of the two main categories of these theories: territorial jurisdiction theory. The second section only includes the fundamentals of territoriality principle and its subtypes; whereas under the third section we had to go into a more profound discussion on main *locus delicti* theorems and their implications.

While the third section theoretically reveals the inconsistencies between current territorial theories and cybercrime, to further back-up these findings, in the fourth section we methodically listed the results of applying various territorial jurisdiction theories to content crimes.[35] Our choice of content crimes among several types of cybercrime can be attributed to two important factors: firstly, due to their direct relation with freedom of speech, content crimes are a rather

[35] One of the three main categories of cybercrime are content crimes; such as criminal copyright infringement and child pornography.

controversial topic; secondly, in the field of content crimes, there are multiple court decisions that we could use as examples while trying to prove our point.

Later in the fifth section we deal with the second major category of jurisdiction theories: extraterritorial jurisdiction theories. In this section, in a similar fashion to third and fourth sections we attempted to determine the result of interactions between cybercrime and currently accepted extraterritorial theories.

1. The Concept of Jurisdiction and Its Evolution

Traditionally the term 'jurisdiction' is used to encompass three different powers of a state. These three subtypes of jurisdiction are 'jurisdiction to prescribe', 'jurisdiction to adjudicate' and 'jurisdiction to enforce'.[36] The first to be examined and also the one that has the uppermost relevance to the subject is jurisdiction to prescribe.

Jurisdiction to prescribe refers to the power of the sovereign state to apply its own laws to the actions, statuses or relations of persons through; legislation, executive act, administrative rule or by court rulings. A more simplified and direct definition can be found in Restatement of Foreign Relations Law of the United States the Third, it is described as '*the right of a state to make its law applicable to the activities, relations, the status of persons, or the interests of persons in things*'[37].

Jurisdiction to adjudicate is the state's authority to *"subject persons or entities to the process of its courts or administrative tribunals"*[38]so that the state can trial and see whether any of its laws has been violated. Jurisdiction enforce is the state's authority to *"induce or compel*

[36] Koops & Brenner, 'Cybercrime and Jurisdiction', 2006, p.3

[37] Restatement of Foreign Relations Law of the United States the Third, 1987, §401. (hereafter: Restatement)

[38] Restatement §401

compliance or to punish noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police or other non-judicial action."[39] As it can be seen without jurisdiction to adjudicate or enforce, jurisdiction to prescribe is more or less a theoretical concept; without prescribing law, adjudicating or enforcing is not possible. However, here we must note that, a legitimate claim to prescribe jurisdiction may not constitute sufficient grounds for asserting jurisdiction to adjudicate or enforce.[40]

Throughout the history of law, all three types of jurisdiction claims has been mostly based on territorial boundaries and claims arising thereof. In other words, sovereign states have the power to make criminal laws and render them applicable upon all persons whose unlawful actions transpired within their territories. So the main rule of jurisdiction always has been that, *'states cannot apply their criminal laws to unlawful conducts happening outside of their physical boundaries'*.[41] Foundations of such perspective can be traced back in the past. Before the huge leap of technological advancements of 20th century, *"…crime was small-scale, consisting of unlawful acts committed by one person or a few loosely-associated persons that were directed against a single victim."*[42] The simplistic and local nature of this type of crime made it possible for local authorities to deal with them reasonably effectively since the motivations and types of crime were firmly limited and clear. The emergence of transportation and telecommunication technologies in the last century forced the existing principles to evolve and encompass a new level of mobility and criminal efficacy. With these new technologies, it became possible for a

[39] Restatement §401

[40] *See:* **Chapter** 3

[41] Koops & Brenner; 'Cybercrime and Jurisdiction', p.4,

[42] Goodman & Brenner; p.18

perpetrator situated in country X to commit a crime and easily flee to country Y or to commit a crime against a victim situated in country Y without leaving country X.[43]

The change in zeitgeist gave birth to new principals which allow states to claim extra-territorial jurisdiction. These rules or principles are categorized based on the nature of link between the crime and the state in question. Today, *there are four broadly recognized principles under which extra-territorial jurisdiction is claimed or exercised in cases of international criminal activity*.[44] These are: the active nationality principle, the passive nationality principle, the universality principle and the protective principle.[45] On the other hand, the existing territory-based principles continued to be referred with some updates in order to cope up with the escalating convolution of crime.[46] Here, all these principles shall be scrutinized one-by-one in order to get a better view of the modern concept of jurisdiction.

2. The Territoriality Principle

Territoriality is still the most important and widely applied principle in terms of jurisdiction. In fact in several countries including the USA there is a general presumption against extraterritoriality; meaning that normally national laws of a state only applies within the territorial jurisdiction of that state.[47] Territoriality principle can be broken down into several elements related with locality. These can be; location of acts, location of tools, location of persons, location of the result or location of basically anything that has relevance with the

[43] Koops & Brenner, 'Cybercrime and Jurisdiction', p.4

[44] Walden, Ian, 'Computer Crimes and Digital Investigations', 2007, p.304

[45] Id.

[46] Goodman & Brenner; p.19-20

[47] Proskauer Ch. 25 II 'The Presumption Against Extraterriotial Application of US Law' http://www.proskauerguide.com/law_topics/25/II [Last visited: 30.06.2012]

crime.[48] Some scholars tend to break down territoriality principle into two different theories; as subjective territoriality and objective territoriality and this distinction bears significance.[49] Subjective territoriality can be formulated as follows: if a criminal act is committed within the physical borders of a state that state can claim jurisdiction.[50] Subjective territoriality is the more well-known of the two as it is the more commonly accepted principle and there is little discussion regarding the application of this principle. Objective territoriality, on the other hand, is a theory that focuses on the location of results and is at least as important as the former when it comes to cybercrimes. This principle can be "*invoked where the action takes place outside the territory of the forum state, but the primary effect of that activity is within the forum state."*[51] According to The Restatement of Foreign Relations Law, a state can use objective territoriality when a *"conduct outside its territory that has or is intended to have substantial effect within its territory"*.[52] Objective territoriality is not a 'territorial' theory per se and has obvious connections with passive personality principle.[53] The most basic example given for this situation is a man standing in the territory of country X and shooting at someone standing inside the territory of country Y with a gun. As for cybercrime though, application of this principle creates a major problem, previously mentioned in Introduction section; namely the problem is *"that lawful behavior in the domestic jurisdiction may be categorized as criminal in a recipient*

[48] Koops & Brenner, 'Cybercrime and Jurisdiction', p.5

[49] Menthe, Darrel; 'Jurisdiction in Cyberspace: A Theory of International Spaces', MICH. TELECOMM. TECH. L. REV. 69 (1998); at paragraph 6. Available at <http://www.mttlr.org/volfour/menthe_art.html>

[50] Id.

[51] Id.

[52] Restatement §402

[53] *See:* **Chapter** 2 **Section** 5.1.

jurisdiction"[54] Furthermore, deciding on location of anything requires meticulous investigation since cybercrimes manifest themselves at multiple locations, virtually at the same time.

3. Four Main *Locus Delicti* Theorems and Their Variations

In order to correctly determine the location of a crime, there are four generally applied theories: physical act theory, instrument theory, result theory and ubiquity theory.[55] The act theory considers the location where the offender has completed the physical action to commit the crime as *locus delicti*. There are various interpretations of the theory but no matter what alternative is used, *locus delicti*, by definition is *"always the location of the offender"*; No matter what theory is used, *locus delicti*, by definition is *"always the location of the offender"*.[56] In the case of modern-era crimes, such as cybercrimes and crimes of omission, it is acknowledged that this theory would prove to be insufficient and also is no longer used by most states as such but rather in combination with other theories.[57] The instrument theory focuses on the time span between the beginning of the crime and its completion. This theory states that locus delicti is the place that an instrument used by the offender takes effect, making the existence of more than one *locus delicti* possible.[58] The result theory suggests that, locus delicti is the place where the crime is completed. Ubiquity doctrine on the other hand is a combination of the first three; merging the physical act theory and the result theory and in some variants of the theory also the instrument theory. Basically it suggests that a crime can be considered to be committed at multiple

[54] Walden, Ian; p.297

[55] Wolswijk, H.D.; p.367

[56] Id. p. 368

[57] Id. p. 367

[58] Id.

locations.[59] Here it must be noted that, applying other theories may also end up with finding multiple places but the difference is that ubiquity approach provides greater flexibility for judiciaries compared to others. Nevertheless, since most states[60] use a variation of the ubiquity theory in their respective laws and/or case law, this theory will be examined in depth here.

Ubiquity theory, in general, claims that, '*an offence may be considered to be committed within the territory of a State if one of the physical acts constituting an element of the offence was committed there, or if the effects of the offence became manifest there'*.[61] This formula is as broad as it sounds; cybercrimes frequently have a 'spill-over' effect and therefore they are not confined within a certain country's sphere of jurisdiction under this theory; since every single location that the offender completes a constituting (*or constituent*) element of crime is *locus delicti*.

However, it must be noted that, there are also views that deem basing jurisdiction on non-constituent parts of the crime also possible. These kinds of approaches have found their place in several court decisions[62] and in several statues; such as the United Kingdom Criminal Justice Act of 1993; which provides jurisdiction on the basis of a 'relevant event'.[63] The Act defines a relevant event as *"any act or omission or other event including any result of one or more acts or omissions"*; which means non-constituent elements of crime are also included.[64] Non-constituent

[59] Id.

[60] I.e. Germany § 9 StGB - *Strafgesetzbuch.* English version vailable at: http://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html

[61] Kaspersen, Henrik W.K., Council of Europe Report "Cybercrime and Internet Jurisdiction" p.8

[62] *See: Libman v. the Queen,* Canadian Supreme Court, 1985 as a notable example.

[63] Criminal Justice Act (CJA) '93, s. 2(1).

[64] Id.

elements of crime include preparatory acts and non-constituent effects.[65] For example, if an e-mail message were to send as part of a conspiracy, this would be a non-constituent element and under English law, the court would be able to seize jurisdiction if any 'relevant event' occurs in England and Wales even if all other such events have occurred abroad.[66] The use of such expansion of the crime concept itself is highly questionable. Yet, the increase in the number of this kind of expansionist laws is not surprising; as the general direction in the evolution of jurisdiction has almost always been towards expansion of the sphere of jurisdiction.[67] As long as jurisdiction is perceived as a reflection of sovereignty, it is nothing but natural that states take on approaches that let them enhance their power to claim territorial jurisdiction when their interests are at stake. Though it is essential to underline that wider jurisdictions have been achieved through expanding the aforementioned theories and definitions related thereof. The transformation of crime towards a transboundary notion contributes to this drift, that it has become relatively easier for states to establish a connection between a crime and their territory.[68] Finally, criminal liability is being extended; especially for cybercrimes. Actors being held liable from a particular crime may include the uploader, the downloader, the server owner, the ISP and so on. It is nothing but natural that these real or legal persons are residing in different states. In addition to the problematic consequences this general inclination produces, the answer to the question of when to apply a territoriality doctrine or how to apply it remains obscured also. As jurisdiction claims are shaped by the national laws and/or the case law of a country and as these differ from each other substantially, it is still very difficult to ultimately answer whether a state

[65] Wolswijk, H.D.; p.372

[66] Walden, Ian; p. 302

[67] Kaspersen, Henrik W. K.; p. 10

[68] Id.

can or cannot assert jurisdiction. It is because, regardless of the theory applied, the results will vary depending on how we define the offence itself. [69] Specifically, what we delineate as the beginning of the offence, the end of the offence or the effects of the offence indirectly shapes *locus delicti*. Therefore, the lack of harmonization of cybercrime laws also contributes to the problem of using territorial jurisdiction theories.

The relation between jurisdiction and non-constituent elements of crime are further examined throughout the thesis; but still it is safe to say here that most of the time the importance or strategic value of asserting territorial jurisdiction based solely on non-constituent elements is low; but on the contrary, the harms of doing so is relatively high, that it is punishing foreign citizens simply because they are operating on the Internet instead of other communication or publication mediums.[70] In order to illustrate and support this claim, the example of content crimes will be scrutinized here.

4. Extended Territoriality and the Problematic Case of Content Crimes

4.0. Why Content Crimes?

In the case of content-related offences objective territoriality and similar extensive territorial approaches are particularly problematic[71] and there are three distinct reasons behind this. Firstly, the level of consensus on contents that are to be criminalized is very low and therefore the act is not illegal in both countries most of the time. Secondly, due to the nature of content crimes, it can be argued that they affect very large number of victims from different parts of the globe simultaneously; possibly enabling many countries to assert jurisdiction to prescribe.

[69] Wolswijk, H.D.; p. 371

[70] Walden, Ian; p.304

[71] Id.

And finally, deciding on the location of both constituent and non-constituent elements of a content crime is relatively difficult to locate compared to other forms of computer or cybercrime.

4.1. Analysis of the Act Theory

In Germany there are two opposing views among scholars and lawyers on this subject. The first and group, which defends a quite restrictive approach, argues that content crimes[72] "*do not have a location of criminal result in the legal sense of the… StGB but instead have only a location of criminal act"*.[73] If we apply the act theory to content crimes, the real difficulty is in answering the question "what is the act that constitutes the publishing or making the content accessible?" Obviously there are two phases of communication via the Internet: uploading and downloading. Predictably, the real fuss is about whether accepting the act of the downloader as a constituent part of publishing or not. The restrictive German approach not only rejects the responsibility of the downloader but also claims that German criminal law cannot be applied to foreign actors located outside of Germany in respect to content crimes.[74] On the other hand, in the notable *Waddon*[75] case, English judges concluded that there are two separate acts of publishing in these cases: *"the first when the data is uploaded to a website, carried out by the perpetrator; the second when it is subsequently downloaded, carried out by the victim"*.[76] This conclusion and thus the decision were based on the Obscene Publications Act 1959. The act gives the definition of the term 'publication' under section 1(3) and specifically sub-sentence

[72] The German Law uses the term 'abstrakte Gefährdungsdelikte'; a term that includes *"making accessible pornography, glorifications of violence or racist or national-socialist hate speech".* Koops&Brenner, 'Cybercrime and Jurisdiction', p.189

[73] Koops&Brenner, 'Cybercrime and Jurisdiction', p.190

[74] Id.

[75] *Regina v. Graham Waddon 1999*

[76] Walden, Ian; 303

1(3)(b) encompasses transmission of data when the data is stored electronically.[77] However, it is important to point out here that, actually under 1(3)(b) the law states that *"a person publishes an article*[78]*…* [is] *who… **transmits** that data"*.[79] The Oxford dictionary defines the verb 'to transmit' as: 1. "*cause something to pass on from one person or place to another"*; 2. *"broadcast or send out (an electrical signal or a radio or television programme)"*[80]. Since data is transferred with electrical signals in the cyberspace, it is almost certain that the latter definition is more suitable in this context. This definition of the word indicates a second party, a receiver who **receives** the transmitted data. In the wording of the law there is absolutely no reference to the receiver, in our case, to the downloader; who most certainly does not transmit the data containing the obscene material. Furthermore, 1(3)(b) has been last amended in 1995 to cover electronic data transmissions and therefore it is questionable that whether the lawmakers had foreseen the currently massive scales of Internet trafficking. Keeping this in mind, *Waddon* case can be shown as the prime example of the abovementioned extension of definitions in existing laws.

Even if the crime were to be considered to have constituted at the location where the material is uploaded, locating the act of upload is still difficult. Brenner and Koops wrote, *"if the content provider is in country A while the hosting provider is in country B; in that case, the act of uploading is initiated in A and terminated in B, and it may even be considered to occur in the intermediate countries through which the data is transported… [it] may also be considered to*

---

[77] Walden, Ian; 302

[78] The law defines the term 'article' as '*any description of article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures'.*

[79] Obscene Publications Act, OPA 95, http://fds.oup.com/www.oup.co.uk/pdf/bt/hedleyaplin/part_a.pdf

[80] Oxford Dictionaries Online; http://oxforddictionaries.com/

take place at the location of the host computer where the material is actually located".[81] The formula which the act theory proposes does not really work in these kinds of cases due to the high number of unknown variables and we believe it should be refrained from.

4.2. Analysis of the Instrument Theory

In the case of applying the instrument theory to a content crime we must also define the instrument(s); as the generally accepted principle is 'states can assert jurisdiction if the instrument crosses through its territory'.[82] It should be considered inappropriate to accept that every computer with access to internet via fiber-optic cables that are transmitting the electromagnetic signals of a content crime, as a basis for asserting jurisdiction; otherwise the instrument is technically taking effect in the entire world.

Similarly, on the topic of satellite communications, the drafters of the Convention on Cybercrime first considered but then discarded the idea of a special clause for satellites, noting that *"in many cases there would be no meaningful nexus between the offense committed and the state… because a satellite serves as a mere conduit for a transmission."*[83] If we are going to accept that satellites are merely devices and not a strong basis for asserting jurisdiction then we also need to stand against very broad jurisdictional claims such as the USA definition of 'protected computer'.[84]

---

[81] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.15

[82] Wolswijk, H.D.; p.370

[83] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.28

[84] *See:* **Section 5.3**

4.3. Analysis of the Result Theory

The second group of scholars in Germany that support an extensive approach claims that, *"a 'location of the criminal result' is given at* all *places where the abstract danger could materialize."*[85] This implies that a person acting outside Germany, *"would not only be liable under German law* [for his relevant act] *but also if this content could be accessed on a foreign server even though the material has no connection whatsoever with Germany."*[86] This means a similar vague situation arises also from the application of the result theory; the Internet is accessible from any country on the world, so the content crime will be viewable by persons from almost every country in the world which leads to an undesirable universal jurisdiction[87] claim for Germany and other countries with parallel views.[88]

4.4. Location of the Victim

Another option could have been determining the location of the victim. Conventional crimes usually take place at the location of the victim; however with cybercrime and especially with content crimes reaching to such conclusions is misleading since most of the time victims are located in several countries. *"For instance, hate speech targeted at Jews supposedly victimizes all Jews, but should this mean that any country with a hate-speech provision and with resident Jews can claim jurisdiction?"*[89] Ian Walden took the example one step further and wrote, *"Even where the perpetrator and victim are located in the same jurisdiction, relevant evidence may*

---

[85] Koops & Brenner, 'Cybercrime and Jurisdiction', p.190

[86] Id.

[87] *See:* **Section 5.4**

[88] Wolswijk, H.D.; p.371

[89] Brenner & Koops, 'Approaches to Cybercrime Jurisdiction', p.17

reside on a server located in another jurisdiction, such as a Hotmail account."[90] As a matter of fact, location of the evidence bears significance when it comes to determining which country has the jurisdiction or in the case of more than one state competing for jurisdiction, which of them has the priority.[91] Therefore the location of the victim does not provide us a significant clue either.

4.5. Location of the Server and the Webpage

On this very issue Menthe wrote, *"…if a webpage is located at Stanford, it is difficult to decide for jurisdictional purposes whether a Bolivian accessing it comes to Stanford or the webpage 'travels' to Bolivia".*[92] Although webpages have no actual location and it is even questionable that they actually exist before they are accessed and appear on the screen of the downloader,[93] this question is important as it bears more figurative implications.

Here a comparison between corporeal and incorporeal content is in order to illustrate the discrepancy of assuming that a website actually travels places for jurisdictional purposes. For example, German law draws the line for child pornography at the age of 14. [94] Obscene pictures of a 17 year old, on the other hand, are considered as child pornography in the Netherlands and therefore being in possession of or disseminating such a picture can be prosecuted in the Netherlands. However if a Dutch were to physically travel to Germany, which would be fairly easy for him since Germany is a neighboring EU country, he could acquire such a picture and the act would be perfectly legal for both the supplier and the Dutch since the act of "making

[90] Walden, Ian; p. 297

[91] *See:* **Section 6**

[92] Menthe, Darrel; at 29

[93] Id.

[94] Brenner & Koops, 'Approaches to Cybercrime Jurisdiction', p.1

available" or "distributing" is not within the Netherlands. The same logic shall apply for contents in incorporeal form.

Therefore we believe there is a vital difference between retrieving or **pulling** the data from a server or actively sending the data or **pushing** it into a computer system via forwarding e-mail or similar methods.[95]

Some scholars have actually considered allocating the virtual content of the webpage to the physical location of the server that constitutes the webpage; i.e. assuming that a website is located in Japan because the data constituting it is in a server in Japan. However we agree with Ulrich Sieber that *"this concept is no longer suitable for global cyberspace."*[96] First of all, today a single website can include data from several servers, which can be located in different countries. Secondly, there have to be a distinction between 'pulling' and 'pushing' data.

Sieber, in his analysis of current German law, argues that if there is only 'pulling' (or downloading - recalling the English court decision in *Waddon*), then *"an application of German criminal law to foreign providers of web pages, located for instance on American servers, would not be reasonable."*[97] We must say that he does not support a system where law of the server's owner prevails no matter what and goes on to say that; "*a general rejection of any domestic* [German] *jurisdiction in these cases is not convincing."*[98] In other words, he suggests that, giving up all jurisdictional claims just because the server is foreign-owned is not the way to go here; however the location of the servers does mean something. We also do not believe in the merits of a system where states prescribe jurisdiction only when the content is stored in a

[95] Koops & Brenner, 'Cybercrime and Jurisdiction', p.200

[96] Id. p.206

[97] Id. p.201

domestic server. This is simply because offenders can use foreign websites to circumvent the reach of law and intentionally address domestic Internet users.[99] In the light of the discussion above, while answering Menthe's question we assume that the Bolivian is 'going' to Stanford, at least in the case when someone is 'pulling" the data in order to protect the uploader who has no intent to "send" the material to Bolivia in the first place.

4.6. Sovereignty and Content Crimes

In response to this conundrum some states not only criminalized but simply blocked the access of their citizens to the outlawed domains by using technical means. In USA the infamous 'Communications Decency Act' (CDA) of 1996 came to force but shortly after was declared unconstitutional by the Supreme Court. However more recent examples of such approach are existent; for example, in 2007 Republic of Turkey enacted the 'Act on Regulating Publications over the Internet and Combating Crimes Committed via These Publications' [100] which endows the ability of blocking access to both foreign and domestic websites which include content crimes to a governmental organization. Obviously such censorship powers can easily be abused and we do not intend to promote such an approach. However, while the notion of sovereignty allows states to take such action, it is difficult to say the same thing for asserting jurisdiction over foreign uploaders and servers. Darrel Menthe, on CDA, wrote the following: *"Quite apart from the internal limitations of the U.S. Constitution, there is little doubt that, under international law, the United States has the jurisdiction prescribe law regulating the content of what is uploaded*

---

[98] Id. p.206

[99] Koops & Brenner, 'Cybercrime and Jurisdiction', p.206

[100] Act Number 5651: "Law on Regulating Broadcasts over the Internet and Combating Crimes Committed via These Broadcasts" (2007) Due to its long name it is usually referred as the Law 5651.

from United States territory."[101] States indeed have the legitimate power to punish an uploader that breaches the law within their territories or block access to certain content; however we believe sovereignty is still tightly connected with territoriality and the link between the uploader and the state is too weak make an exception to this premise. Recalling the Restatement, we can say that, most of the time, neither the act of the uploader has any substantial effect nor does the uploader intend to have such an effect in a specific foreign country. Invoking objective territoriality shall require a unique interest in comparison to the other states where the content is also downloadable.[102] Only if the content is targeted at a specific state or its citizens and a provable substantial impact occur subsequently after the publishing of such content then that state should be able to assert jurisdiction. Accepting otherwise theoretically imbues the state that has the strictest laws with the ability to prescribe its laws to the entire Cyberspace; resulting in major limitations to freedom of speech in Cyberspace.

If the victim of a content crime is the public in general, that the content crime is allegedly encouraging potential offenders,[103] it is reasonable to expect from any state that asserts jurisdiction based on objective territoriality to first scientifically prove that such content actually did have an impact within its territory.[104] Failing to do so will obviously undermine the strength of claims based on 'substantial effect'. If the victim of the crime is someone else, such as the under-aged person(s) that appears on a pornographic picture, we would end up with applying the same *locus delicti* theorems that lead us to extreme outcomes.

---

[101] Menthe, Darrel; at paragraph 16

[102] Menthe, Darrel; at 28

[103] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction' p.17

[104] Id. p.18

Several other reasons can be listed to demonstrate why objective territoriality is intrinsically unsuitable for content crimes; yet neither that is the main focus of this thesis nor does that deny the usage of objective territoriality principle for other types of cybercrime. Such analyzes for different types of cybercrime will be made in the later chapters but before doing so extraterritorial jurisdiction theories should be examined as well.

5. Extraterritorial Jurisdiction Theorems

5.0. The Purpose Behind Extraterritorial Jurisdiction

As it was mentioned under **section 1**, extraterritorial jurisdiction theories are traditionally considered as exceptions to the main rule, which is the territorial jurisdiction principle and therefore are usually limited to specific conditions and/or specific crimes. Therefore the most important thing that should be realized about extraterritorial theories is that, these theories were originally created to be resorted only when no territorial theory is suitable and/or applicable. Walden categorizes extraterritorial theories into two groups; as those that are reflecting an inward focus and those with an external focus.[105] According to this, while passive nationality and protective principles are there to safeguard national interests, active nationality and universality principles are helping the global fight against certain crimes and rely on international cooperation.[106] We believe that with the effect of the increasingly expansive jurisdictional theories, this conventional categorization is no longer accurate and we tried to illustrate that through this section. However this distinction is still important that it shows us the original function of these theories and the reasoning behind them so that the current legal landscape can

[105] Walden, Ian; p.304

[106] Id.

be analyzed from a 'purpose' perspective. Also later in **section 6** we will refer to this distinction while we discuss the relative strengths of these claims.

5.1. Passive Nationality Principle

Passive nationality theory considers the nationality of the victim as a constituting factor while deciding on jurisdiction.[107] As it was mentioned under **the Territoriality Principle**, this theory is highly similar to the objective territoriality approach however the two principles are not interchangeable; the difference with passive nationality is that the state is asserting to protect a national located outside of the state's territories. Invoking this principle is subject to different requirements in various states. In Germany either the crime has to be punishable in the state it was committed or no criminal jurisdiction should apply to the crime where it was committed to resort to the passive nationality theory.[108] In the United States, at federal level, usage of passive nationality is limited to crimes that are targeting a department of the government.[109] 18 U.S. Code § 1030 reads as follows under (a) (3): *"whoever… intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government… shall be punished…"*[110] Similar approaches can be found in individual state laws also; such as Michigan claims jurisdiction over crimes victimizing government agencies or agents –both legal and real persons.[111]

---

[107] Id.

[108] §7 Nr. (2)1. StGB - *Strafgesetzbuch*

[109] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.25

[110] 18 U.S. Code § 1030 (a)(3)

[111] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.25

Whereas these are general criminal laws not specific to cybercrime, they are not excluding cybercrime either. Content crimes again lead to interesting results in the event of invoking passive nationality theory similar to the ones caused by expansionist territorial approaches. If the content crime offends a group of people that has members all around the world, may every country that has implemented passive nationality principle assert jurisdiction, claiming that one of their citizens is a victim? The same question can be asked for virus attacks where the perpetrator does not seemingly target a specific individual but still affects thousands.

Since the function of passive nationality principle is protecting the citizens of a state while they are abroad, the answer to this question is mostly related with the national laws of the state where the victim is located in at the time of crime. As German law suggests, if the forum state has also criminalized the act and also has the capability and the will to exercise jurisdiction, invoking this principle is redundant and has no positive consequence of any kind and therefore should be avoided. This has two reasons: first, almost always the perpetrator will not be present within the country and initiating the prosecution without the perpetrator is not possible; second, it can be considered offensive to override the territorial jurisdiction of another state for a crime where there is no consensus on.[112]

On the contrary, if no such jurisdiction is available, passive nationality can be an option for these types of cybercrime. However in this case, since there are numerous victims, the intended target (if any) may constitute a factor while deciding on jurisdiction. In the renowned *Yahoo!* case[113] one of the foremost factors in the decision was *"the perceived targeting of*

[112] Menthe at paragraf 10

[113] *See:League Against Racism and Anti-Semitism, French Union of Jewish Students v. Yahoo! Inc. (USA), Yahoo France,* Tribunal de Grande Instance de Paris, 2000

French citizens".[114] This case of course is not an example of invoking passive nationality as the citizens were in France at the time of the crime and therefore the French court simply asserted jurisdiction on the basis of territoriality; however the idea can still be borrowed. Doing so would imply the possibility of looking into targeted viewers before asserting jurisdiction based on the nationality of the victim. If we set nationality of intended viewers as a criterion it might be possible to reduce the chances of content owners or publishers being victimized by foreign jurisdictional verdicts. However in a substantial number of cases deciding on the intended viewers may still prove to be challenging. The language of the content might provide insight for some cases where the language is strongly tied to a single state or a small set of states. Another indicator of the intended viewers might be clear references to a specific country or countries.

5.2. Active Nationality Principle

Active nationality theory takes the nationality of the perpetrator as a basis for exercising jurisdiction and is widely recognized as the second most important basis of jurisdiction for cybercrime after territoriality.[115]

German Criminal Law uses active nationality principle in a similar fashion to passive nationality principle. When a crime is committed abroad by a German national, German courts have jurisdiction as long as the crime is **also punishable** in that country or state or if the crime is not subject to any criminal jurisdiction where it was committed.[116]

In the United Kingdom extraterritorial jurisdiction theories has been altogether rejected traditionally until recent times; but for a certain set of crimes, including some types of

[114] Walden, Ian; p. 303

[115] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.24

[116] §7 Nr. (2)1. StGB - *Strafgesetzbuch*

cybercrime, this position has been changed.[117] The Sexual Offences Act of 2003 implements the active nationality principle for sex-related offences including child pornography with the condition that the act is **also punishable** in the country or territory it was committed in.[118] Nevertheless, this law remains as an exception and there are strong arguments (such as difficulty of gathering evidence and extraditing the suspect) against using active nationality principle for other crimes.[119]

While double-criminality is generally accepted as a basis for extradition in several jurisprudences, under clauses related to active nationality we see it as a basis for jurisdiction. Not surprisingly, while the active nationality theory is regarded to have an external focus; it proves to be rather competent with cybercrime. First of all, lack of harmonization in cybercrime laws ceases to be an issue with the implementation of double-criminality principle. Also, a great majority of the time, there is nothing unclear about the nationality of the perpetrator; except for DDOS[120] attacks. Yet the most important feature of active nationality is that, at least in theory, it lowers the possibility of cybercriminals getting away without even being prosecuted due to lack of legislation or will to do so. We can argue that when a state invokes an extraterritorial jurisdiction theory, there is *prima-facie* evidence of state's willingness to prosecute the crime; especially when the invoked theory has an external focus. The reasoning is that, in these cases neither the state nor a citizen of it receives direct harm from the crime in question. Thus, widespread adaptation of this theory could have helped given that extradition is not a problem

[117] Walden, Ian; p.304

[118] Id.

[119] Id. p.305

[120] DDOS (Distributed Denial of Service) attacks prevent legitimate users from gaining access to their web space by bombarding access gateways with a barrage of data. Wall, S. David; *'Cybercrime' p.222*

and both states are cooperative; but as mentioned earlier, such presumptions can be considered unreliable.

5.3. Protective Principle

Protective principle suggests that, a state should have jurisdiction when a criminal act that is committed beyond its borders is targeting the national security or general interests of that state. The common examples for exercising protective principle include acts of espionage and counterfeiting.[121]

A notable example that specifically mentions cybercrime is the USA Patriot Act of 2001 which amended the Computer Fraud and Abuse Act[122] and extended the jurisdiction to include computers **outside** the United States but 'used in a manner that affects interstate or foreign commerce or communication of the United States'.[123] With this amendment the United States can now use domestic procedures to join in international hacker investigations more often; as hackers in other countries route communications through the United States frequently even when the targeted computer is in a state irrelevant to the USA.[124] Undoubtedly this addition is strengthening the international cooperation since it will allow the US government to prosecute criminals of its allies. However the same amendment can also cause jurisdictional conflicts with states which the USA has poor diplomatic relations with.

[121] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.26

[122] 18 USC § 1030(e)(2)(B)

[123] Walden, Ian; p. 301

[124] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p. 27

5.4. Universality Principle

Universality principle provides a state with an ultimately wide jurisdictional claim; unlike none of the principles mentioned until now, a state can assert jurisdiction with universality even when none of the constituent or non-constituent elements of the crime has relevance with that state. According to the Restatement states claim universal jurisdiction for a few offences *"recognized by the community of nations as of universal concern."*[125]

Germany claim universal jurisdiction for a handful of crimes including attacks on air and maritime traffic, human trafficking, drug dealing and child pornography.[126] Whereas it is doubtful that individual states of USA can ever exercise universality, the federal government does so for a number of crimes including piracy, hostage-taking, aircraft hijacking and torture.[127] The United Kingdom, in a similar fashion, claims universal jurisdiction over crimes such as genocide and piracy.[128]

We believe that the definition in the Restatement implies that a majorly unified crime description is required in order to claim universal jurisdiction. Ian Walden also wrote that universality principle is "*for crimes broadly recognized as being crimes against humanity*".[129] This makes us question the aptness of the universal jurisdiction claims of Germany and some other countries like Belgium regarding child pornography. While we understand the concerns towards the dissemination of child pornography and accept that *"child pornography is already*

[125] Restatement § 404

[126] §6 Nr. StGB - *Strafgesetzbuch*

[127] Restatement § 404

[128] Walden, Ian; p. 304

[129] Id.

an almost universally outlawed activity";[130] we fail to see an almost universal consensus on the definition of 'child pornography'. For example, whereas some states such as the United Kingdom or the Netherlands consider obscene 'pseudo-photographs' or computer generated images of minors as child pornography, some states such as Turkey[131] or Japan[132] do not. Thus we believe such universal claims regarding cybercrime or computer crimes are somewhat premature.

Chapter 3: Conflicts of Jurisdiction and the Dispute of Priority

0. Intro

Although various jurisdictional problems seem to be inevitable in the case of cybercrime, criminal law possesses an integral 'checks and balances' mechanism to alleviate some of these issues and provide guidance in sorting out any kind of jurisdictional conflicts between states.

First of all, even though we have referred to the term 'jurisdictional conflict' previously; we deemed an in-depth explanation of the term is essential before proceeding to the dispute of priority and thus we dedicated the first section of this chapter to examining jurisdictional conflicts.

---

[130] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p. 36

[131] Art. 226 Turkish Criminal Code. TCK - *Türk Ceza Kanunu*,

[132] Act No.52 of 1999, Art. 7. Japan is a major producer of child pornography and second biggest consumer after the USA. Japan also has not banned the possession of real child pornography either. Distribution and production however are illegal since 1999.

In order to solve jurisdictional conflicts some guiding principles have been implemented into national statues and some have been laid down as non-binding guidelines by scholars[133] or international organizations[134].

In the second section of this chapter we first analyzed the factors given in the national laws and discussed on the manner they should be construed for cybercrimes. We mostly looked into the United States law for two reasons: 1- Whereas the UK and Germany have not incorporated a list of factors in their respective national codes, the list given in the Restatement includes numerous principles and commentaries on them and without doubt is the most comprehensive guide among all national laws; 2- Partially because of this legal vacuum, some of the principles listed in the Restatement later has *"emerged as a principle of international law as well"*.[135] After this extensive analysis, under section three, we briefly looked into the laws and bilateral agreements of the United Kingdom and Germany that provide some guidance in the matter.

Finally in the fourth section we analyzed other guidelines drafted by NGOs or universities that suggest factors in prioritizing jurisdictional claims and also, while doing so, we discussed the practicality of these factors from cybercrime perspective.

1. Jurisdictional Conflicts

Traditionally, conflicts of jurisdiction are categorized into two; as negative and positive conflicts. A negative jurisdictional conflict refers to a situation in which not one country claims

---

[133] Princeton Project on Universal Jurisdiction, *The Princeton Principles on Universal Jurisdiction*(2001). Available at: <http://www1.umn.edu/humanrts/instree/princeton.html>

[134] *See*: **Section 3** of this Chapter.

[135] Restatement § 403 Comment (a)

jurisdiction over a crime.[136] Considering our findings in the prior chapters, it is safe to say that negative conflicts are very unlikely to happen with the cybercrime but still a possibility that cannot be neglected. It would be a plausible scenario, *"if the perpetrator acts from a cybercrime freehaven, and if she is a national of that country"*.[137] Nevertheless we think negative conflicts in cybercrime will most likely arise from the unwillingness of states to assert jurisdiction; not because they cannot find any grounds to do so.

Conversely, a positive jurisdictional conflict is highly likely due to the *"law reforms that extend territorial jurisdiction and establish extra-territorial jurisdiction as a policy to the* [cybercrime] *phenomenon"*.[138] On the other hand, *non bis in idem* principle does not allow an alleged perpetrator to be prosecuted more than once for the same criminal act. Multiple investigations create a significant inconvenience on the offender's side as it will mean *infringement of his* [the perpetrator's] *privacy and privacy-related interests*.[139] Furthermore, resolving positive jurisdictional conflicts early will prevent *"duplication of effort, unnecessary inconvenience for witnesses, or competition among law enforcement officials"*.[140]

Resolving a jurisdictional conflict will require the contribution or therefore communication of all sides of the conflict. Likewise, according to the Cybercrime Convention, in the case of a positive conflict, *"…Parties involved shall, where appropriate, consult with a view to determining the most appropriate jurisdiction for prosecution."*[141] However the Convention

[136] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p.40

[137] Id.

[138] Walden, Ian; p. 306

[139] Koops & Brenner; 'Cybercrime and Jurisdiction', p.16

[140] Explanatory Report on Convention on Cybercrime, paragraph 239 (A). Available at: <http://dasalte.ccc.de/cybercrime/mirror/FinalCyberRapex.htm>

[141] CCC Art 22 (5)

does not provide the Parties with the details of this decision-making process; we do not know the protocol to be used for such negotiation and the criteria for deciding on 'which jurisdiction shall prosecute?'[142] All in all, there are no internationally agreed binding criteria in this subject.[143] Nevertheless, as we have mentioned under Intro, various rules can be found in national laws or scholarly writings.

2. Reasonableness Standard in the Restatement

2.1. When Exercising Jurisdiction to Prescribe

Most of the time, the universal principles that governs claims of jurisdiction are altogether named as the 'standard of reasonableness'. Every jurisdiction claim should be in accordance with reason in order to avoid abusing territorial jurisdiction claims. Previously we have mentioned various theories that provide grounds for states to exercise jurisdiction; but they may be insufficient and annulled if the reasonableness criteria are not met. According to the Restatement main factors contributing to this assessment are: [144]

> *a) The link of the activity to the territory of the regulating state, i.e. the extent to which the activity takes place within the territory, or has substantial, direct and foreseeable effect upon or in the territory.*
>
> *b) The connections, such as nationality, residence or economic activity, between the regulating state and the person principally responsible for the activity to be regulated, or between that state and those whom the regulation is designed to protect*

[142] Walden, Ian; p. 307

[143] Id. p. 309

The first two factors are simply an acknowledgement of territorial and national bases for jurisdiction to prescribe. However, we must note that the factors listed here are not in a priority order and all contribute at an equal level for an evaluation.[145]

> *c) The character of the activity to be regulated, the importance of the regulation to the regulating state, the extent to which other states regulate such activities and the degree to which the desirability of such regulation is generally accepted.*

We believe some of the most important factors are listed here in paragraph (c); since it clearly states that type or character of the activity to be regulated and general acceptance of such regulation are vital. Some of our previous arguments are against legal practices which we conceive as in contradiction with this principle. Moreover, we think that this paragraph should be read and understood together with the paragraphs (e) and (f) for a correct interpretation.

'Character of the activity' and 'importance of the regulation to the regulating state' are factors that are somewhat difficult to justly implement due to their subjective nature. An assessment made in respect to this factor should not be related to the general and abstract opinion on a type of crime but rather both country specific and case specific. An example would be the German criminal law that prohibits glorifying national socialist regime.[146] In a scenario where a German national commits various incitement to hatred crimes, including national socialist propaganda, by forwarding e-mail to recipients in both Germany and Turkey, while residing in Turkey, we can assume that Turkey and Germany have both asserted jurisdiction. If Turkey prosecutes, it will either treat national socialist propaganda as any other incitement to hatred

---

[144] Restatement § 403 (2)

[145] Restatement § 403 - Commentary (b)

[146] §130 Nr. (3) and (4). StGB - *Strafgesetzbuch*

crime or ignore those parts of the criminal conduct, since there is no specific clause in Turkish Criminal Code that mentions glorifying national socialism. We can argue that the importance of regulating crimes related to National Socialism is significantly higher for Germany than regulating other incitement to hatred crimes and that Germany should prosecute due to its special interests here. Conversely the other two factors; 'the extent to which other states regulate such activities and whether such regulation is generally acceptable', limit the application of the first two. If we apply these factors too, we will see that several other states have forbidden material with NAZI party and National Socialism in general to different extents[147] and we can insist on our argument that Germany should prosecute. However a conclusion should not be hastily reached; because drafters of the Restatement have placed relatively more objective factors to further balance the outcome of factors discussed in here, in the paragraphs (e) and (f).

d) The existence of justified expectations that might be protected or hurt by the regulation.

The term 'justified expectations' may include a broad range of expectations; such as those of the public, the victim, the perpetrator or third persons somehow involved in the conduct. We believe the most important expectations and the ones that we should be focusing on are those of the victim and the perpetrator. These two sides can have common interests as well as conflicting interests. I.e. fair trial is theoretically in the interest of both sides. A commission working paper on the subject[148] defines the primary interest of victims as participating in the

[147] In the respective laws of several European countries including Italy and France and also in Israel there are restrictions on owning or distributing national-socialist material.

[148] Commission of the European Communities, Commission Staff Working Document; Annex to the Green Paper 'On Conflicts of Jurisdiction and the Principle of ne bis in idem in Criminal Proceedings' (2005) 1767; Section 9.3.

trial. The paper ties this to the "*legal, financial, linguistic and psychological burdens"*[149] which a trial in a foreign country may impose on the victim. Victims also have a justified expectation that the crime will be extensively and efficiently prosecuted. This is not only in the interest of victims but also in the interest of law and in the case of cybercrime this might grant an advantage to the state that has a higher technical capability that can conduct the prosecution with greater prowess.

On the other hand, *"the victim's interests are by nature one-sided and need to be…balanced"*[150] with the interests of the perpetrator/defendant. In accordance with *nulla poena sine lege,* we can argue that perpetrators usually have a justified expectation to abide by none but the laws of the territory they are located in. We agree with the drafters of the paper that neither side's interests qualify as a 'first rank' criterion but that they might be given a second or third rank priority.[151]

e) The importance of the regulation to the international political, legal or economic system.

f) The extent to which the regulation is consistent with the traditions of the international system.

Many states criminalize contents that only have domestic or regional significance to protect public order whereas such contents are not deemed illegal or dangerous by a great majority of the international community. In cases where the law is irrelevant to a substantial majority of the international community, we may assume that the importance of the regulation to the international system is relatively lower. Following our previous example regarding national

[149] Ibid.

[150] Ibid.

[151] Ibid.

socialist hate speech, we can argue that prevention of promotion of National Socialism holds an international value and safeguards democratic and humanitarian values laid down in various UN documents[152] and thus it is both important for international legal system and in accordance with traditions of the international system. There might be other relevant factors to consider in our example case but still it is safe to say that Germany will most likely have the upper hand in this comparison.

g) *The extent to which another state may have an interest in regulating the activity*

h) *The likelihood of conflict with regulation by another state.*

The last two paragraphs shall be construed in the light of the comments and reporters' notes. According to the commentary regarding section 403, if a state has already exercised jurisdiction, it might be considered by other states as a reason under (g) and (h) to refrain from regulating; however this is not conclusive on its own; under Reporters' Notes it is stated that, if the interests of more than one state are competing then the court shall do the weighing of interests and decide on jurisdiction afterwards.[153]

Reasonableness standard is checked for every state's claim; even if there is only one state asserting jurisdiction. After this analysis if there is still more than one reasonable claim then we need to pass a judgment and answer the question: 'For which state is it more reasonable to exercise jurisdiction?' This is indeed a difficult task as there is no clear line here that we can

[152] *See:* United Nations General Assembly Resolution A/66/460 on "Inadmissibility of Certain Practices That Contribute to Fuelling Contemporary Forms of Racism, Racial Discrimination, Xenophobia and Related Intolerance." (2011)

[153] Restatement § 403 – Reporters' Notes, 6.

draw to come up with an abstract and general rule; instead reasonableness is a balance mechanism that requires us to analyze every offense individually.

The Restatement also notes that, if there is a clear difference between the strength of claims, a state should self-evaluate and defer to the state with the highest interests.[154] Koops and Brenner wrote that, an example to such a clear difference would be a case where an offender in country A commits an act of fraud against a victim in country B by using a computer system. This scenario ends up with the clash of the territoriality claim (location of act, perpetrator and tools) of country A and territoriality claim (location of victim and results) of country B.[155] According to the authors, country A's interest in exercising jurisdiction is *"subordinate to country B's interests"* and *"country B's interest is clearly greater"*.[156] While we agree that location of the victim and results are the stronger arguments for prescribing jurisdiction, we also believe that type (character) of the crime is an equally imperative factor in this evaluation and if there was no agreement on the nature of the crime between the countries A and B, reaching to a conclusion would be more difficult. Koops and Brenner also agree that in a case where act is legal in A but illegal in B there is no straight answer.[157] Furthermore, from the perspective of jurisdiction to adjudicate additional factors may affect our reasoning and also the result.

2.2. When Exercising Jurisdiction to Adjudicate

Early in the thesis we have noted that jurisdiction to prescribe has practical effects only when coupled with jurisdiction to adjudicate and enforce. The Restatement includes a similar set of criteria to help American courts deciding in if it is reasonable to exercise jurisdiction to

[154] Restatement § 403 (3)

[155] Brenner & Koops; 'Approaches to Cybercrime Jurisdiction', p. 31

[156] Id. p. 33 and 34

adjudicate. We will not examine these one by one since some of them are very similar with the above-mentioned principles for jurisdiction to prescribe; nevertheless there are a couple of items distinctive on the list which we will elaborate.

First of these is whether the person or thing related with the activity is present in the state. This is simply because a state's exercise of jurisdiction to adjudicate with respect to a person or thing is not practical while the person or thing is not physically located in the state as it will require extradition of the person or transfer of the thing. In some guidelines and legal doctrine this factor is also mentioned as 'custody of the perpetrator'.

An Australian court decision[158] is remarkable in this respect. The case was regarding an Australian man harassing and stalking a Canadian woman who lives in Toronto via phone calls, letters and e-mails. Eventually a Magistrate in Melbourne received the case and decided that the crime occurred in Canada where the victim was located and refused to exercise jurisdiction to adjudicate; the Supreme Court of Victoria ruled that, even though the effects were felt entirely in Canada, the Australian courts still did have enough grounds to establish jurisdiction on, due to the perpetrator's presence in Australia and reversed Magistrate's decision.

We believe inferences of implementing this factor in cybercrime related conflicts would be rather complicated. If this factor plays a major role in prioritizing jurisdictional claims, a situation similar to the ancient approach towards high-seas piracy would arise and cybercriminals could be tried where they are found.[159] Needless to say, despite the hint of resemblance, cybercriminals are not high-sea pirates. When there is a jurisdictional conflict involving a 'real-

---

[157] Id. p. 35

[158] *Sutcliffe,* [2001] VSC 43

[159] 'Ubi te invenero, ibi te judicabo'. Brenner & Koops; 'Cybercrime & Jurisdiction', p.333

world' crime, usually there is a single offense or a single course of conduct that constitutes multiple offenses.[160] Then each state assert their claim on the same criminal activity, *"which presumably occurred in the territory of one and only one country."*[161] Imagine that a Russian terrorist takes ten people with various nationalities hostage at a hotel lobby in Switzerland and wounding three in the meanwhile. Even though the act constitutes multiple offenses there is one course of conduct and every state related to the conduct through nationality, will request the punishment of the same conduct as Switzerland, which has the custody of the terrorist. However with cybercrime, most of the time, each state's claim is based on an activity that can be separated from others factually and legally.[162] Therefore the state that has the custody may only prosecute for the crimes that it deems detrimental to its interests. In a scenario where the terrorist is a cybercriminal instead and he only uses a computer located in Switzerland to steal credit card information from victims located in different countries, connection of Switzerland with the crime would be lower whether or not any of the victims are Swiss. On the other hand, not every cybercrime is like this and some do constitute of a single offence -or a single course of conduct that constitutes multiple offenses- as in the stalking case mentioned above. To sum up, custody of the perpetrator should be weighted less in cybercrime than real-world crimes as a general rule; but in some cases it may be significant.

The other principle worth mentioning here is the consent of the person (perpetrator). From the perspective of the alleged perpetrator, one country's substantial or procedural criminal law may be more advantageous. In instances where more than one criminal code is applicable to an offender, the general principle of criminal law is to apply the law in benefit of the offender.

---

[160] Id. p.334

[161] Id.

Also the offender would probably prefer to be trialed in the country which he is a citizen of. Therefore we believe consent or lack of consent of the alleged offender should be given some weight too.

3. Factors That Determine Priority in English and German Laws

English law does not provide an explicit statutory guidance on principles or factors to be used in jurisdictional conflicts; however there are some factors mentioned for settling concurrent requests for extradition- which we can refer to due to the similarity between two concepts.[163]

The Extradition Act of 2003 suggests that factors to be taken in these cases are: *"the relative seriousness of the offences concerned"*, "*the place where each offence was committed"*, *"the date on which warrant was issued"* and *"whether, in the case of each offence, the person is accused of its commission or is alleged to be unlawfully at large after conviction"*.[164]

Among these four factors we believe only the first one can be useful towards jurisdictional conflicts involving cybercrime. A comparison in seriousness may depend on the amount of harm the crime inflicted upon the sides of the conflict or the amount of difference between potential sentences or the importance of the regulation to these states. We have already discussed the 'importance of the regulation to the regulating state' factor. 'Harm factor' and 'punishment factor' will be evaluated in the following section so we skip them for now.

---

[162] Id.

[163] Walden, Ian; p. 309

[164] Extradition Act 2003, s 44(7). Available at <http://www.legislation.gov.uk.>

In Germany, the Code of Criminal Procedure under the section entitled, 'Non-Prosecution of Offences Committed Abroad'[165] states that, public prosecutors may dispense with prosecuting criminal offences that have been: committed outside the territorial scope of the statue or committed by a foreigner in Germany while on a foreign ship or aircraft. However this section, while stating that prosecutors 'may' dispense with the prosecution, it does not provide guidance on when the prosecutors 'should' do so and therefore not sufficient for our purposes.

On the other hand, Germany is signatory to many bilateral treaties on extradition and some clauses therein are similar to the UK Extradition Act provisions. For example Germany-USA Extradition Treaty of 1978[166] states that if there are concurrent requests for the extradition of the same offender, the factors that should be considered in the decision are: 'the relative seriousness of the crimes', 'the place of the commission of the crime' and 'the nationality of the offender'.

4. Other Possible Factors That Determine Priority

The guidelines for jurisdictional conflicts which the Eurojust College issued in 2003 also mention the harm factor.[167] The main rule laid down in the Guidelines is that prosecution should be made by the state *"where the majority of the criminality occurred or where the majority of the loss was sustained"*.[168] We believe the 'harm principle' would prove useful in conflicts regarding most cybercrime; such as virus attacks. As Brenner wrote, *"One obvious measure of harm is the*

[165] §153 (c) StPO *Strafprozessordnung*. Available at <http://www.gesetze-im-internet.de/englisch_stpo/englisch_stpo.html>

[166] Germany Extradition Treaty with the United States 1978; available at <http://internationalextraditionblog.com/2011/04/28/germany-extradition-treaty-with-the-united-states/>

[167] Eurojust Annual Report 2003, 'Guidelines for deciding "which jurisdiction should prosecute?" <http://www.eurojust.eu.int>

number of victims."[169] In a major virus attack with massive amount of victims, even without going into monetary calculations of harm, countries will surely be able to display the harm they received by the number of computers infected. Undoubtedly, in cases where harm can be calculated precisely, value of monetary loss is also an indicator of harm.[170] However with some types of cybercrime harm can manifest itself in other forms; such as stealing military technology from a state or crippling its vital systems clearly inflicts a damage that cannot be evaluated by these parameters.

Whereas the harm principle serves as a rule of thumb, Eurojust Guideline mentions several other factors that should be considered; such as: 'the location of the accused and possibility of extradition', 'availability of evidence and witnesses' and 'the negative effect of delay in proceedings on the accused'.[171] Eurojust Guidelines also suggest that the difference between potential sentences in different jurisdictions should not be a primary factor in the evaluation however prosecutors shall not seek to prosecute crimes the jurisdiction where the foreseeable punishment is the highest.[172] The punishment factor is often referred to in the United States when settling jurisdictional conflicts among states;[173] yet we believe it is a factor that should not be regularly brought forward in international jurisdictional conflicts. First of all, determining the amount of punishment is an inseparable part of jurisdiction to prescribe and states should be able to freely decide in that matter. If we consider the amount of punishment as a factor (especially a prime factor) then we will incite all states to raise the sentences in their

---

[168] Eurojust Guidelines, p.62

[169] Brenner & Koops; 'Cybercrime and Jurisdiction' p.337

[170] Id.

[171] Eurojust Guidelines, p. 63, 64 and 65

[172] Id. at p. 65

Criminal Codes and indirectly disrupt their sovereignty. Secondly, since the amount of actual punishment can only be determined after the completion of trial process, sentences determined in national criminal laws do not provide a reliable indicator in such comparison.

One other guideline for jurisdiction has been released in 2001 by a group of scholars, under the name "The Princeton Principles on Universal Jurisdiction'. Similar to the Restatement, there is no ranking among the factors supposedly; but the drafters also acknowledge that some factors would often be more 'weighty' in the assessment.[174] Factors listed here are: 'multilateral or bilateral treaty obligations', 'place of the commission of the crime', 'nationality of the victim and/or perpetrator', 'the likelihood, good faith and effectiveness of prosecution', 'convenience to parties and witnesses' and 'availability of evidence'.[175]

Chapter 4: Convention on Cybercrime, ACTA and the Future of Cybercrime Jurisdiction

0. Intro

So far we have mostly discussed on how national laws from the countries we have selected shape the international cybercrime jurisdiction. At the same time governments took steps aiming to prevent jurisdictional conflicts by unifying their laws at a supranational level.

---

[173] Brenner & Koops; 'Cybercrime and Jurisdiction' p.344

[174] The Princeton Principles on Universal Jurisdiction, Principle 8, Commentary

[175] The Princeton Principles on Universal Jurisdiction Principle 8

In the first section, we wanted to completely scrutinize the Convention on Cybercrime[176] due to our many references to this agreement in the previous sections. We believe CCC is a significant agreement in the field of cybercrime, even with its shortcomings and would have constituted a significant part of this thesis only if it had included more precise provisions on the jurisdiction side of the subject. Furthermore we think that the approach set in CCC has gained strength and influenced another vital agreement: Anti-Counterfeiting Trade Agreement.[177]

In the second section we examined ACTA; an agreement that has been criticized at so many different levels as soon as it became public information. Although ACTA is mainly an intellectual property related agreement, it includes provisions regarding regulating cyberspace, criminal prosecution and international cooperation; which makes the agreement crucially important for the purposes of this thesis.

Finally, in the last section of the chapter and also the thesis, we examined the nature of international cooperation – cybercrime relationship, and questioned its necessity for cybercrime.

1. Jurisdiction in the Convention on Cybercrime

In 2001, in an attempt to harmonize international cooperation regarding the investigation of cybercrimes at European level, the Convention on Cybercrime was introduced. The Convention has been signed by not only member states of Council of Europe but also by Canada, USA and Japan; augmenting its significance by adding a more global attribute.

Article 22 of CCC, entitled 'Jurisdiction', under subsection 1 provides some insight on the subject:

---

[176] Convention on Cybercrime, Budapest 23.11.2001 (Hereafter: CCC)
Available at: <http://conventions.coe.int/Treaty/en/Treaties/html/185.htm>

1. "Each Party shall adopt such legislative and other measures as may be necessary to establish jurisdiction over any offence established in accordance with Articles 2 through 11 of this Convention, when the offence is committed:

a. in its territory; or

b. on board a ship flying the flag of that Party; or

c. on board an aircraft registered under the laws of that Party; or

d. by one of its nationals, if the offence is punishable under criminal law where it was committed or if the offence is committed outside the territorial jurisdiction of any State."[178]

This article is mainly acquainting that states shall adopt the necessary legislations to claim jurisdiction on the grounds of territoriality, flag principle and nationality. Although these principles laid down in the Convention are appropriated here in the exact order, there is neither an implication of a hierarchy of rules nor a mandatory provision. Though under subsection 2, it reads:

2."Each Party may reserve the right not to apply or to apply only in specific cases or conditions the jurisdiction rules laid down in paragraphs 1.b through 1.d of this article or any part thereof."

The indication of this clause is in line with the earlier statement; "territoriality is still the main ground for asserting jurisdiction". On the other hand, information regarding determining *locus delicti* or in other words localizing the crime is not included within the Convention. Last but not least, subsection 4 states that:

---

[177] ACTA, *Anti-Counterfeiting Trade Agreement*, full text available at < http://www.ustr.gov/webfm_send/2379>

4. "This Convention does not exclude any criminal jurisdiction exercised by a Party in accordance with its domestic law."

This sentence effectively reflects the stance of CCC on the matter; that it does not deny Parties from exercising any specific existing principle or approach.

Drafting committee of the CCC has also considered the possibility of implementing *sui generis* jurisdiction principles specifically for cybercrimes; though they rejected this possibility on two grounds.[179] Firstly, simply because perpetrators or the attacked computers/computer systems were assumed to be existent at a certain physical location at the time when constituent elements are fulfilled, regardless of the transboundary effects of the actions and secondly because they concluded that conventional theories are not useless and are applicable also in the case of cybercrimes.[180] In other words, at the time of the drafting, it was deemed unnecessary to develop alternate jurisdiction principles.[181] The legitimacy of these arguments will be further assessed under the Conclusion; yet on the topic of *locus delicti* it can be concluded that despite CCC relies on traditional jurisdiction grounds, especially territoriality; it remains silent on the *locus delicti* theorems.

In Chapter 2, under sections 2 and 3 we have already illustrated the problems created by the extensive *locus delicti* interpretations and theories; that they generate too many jurisdictional claims and possibly lead to positive jurisdictional conflict. In Chapter 3 we have also mentioned that CCC does not provide criteria to determine most appropriate jurisdiction in the event of multiple jurisdictional claims.

---

[178] Art. 22 CCC

[179] Kaspersen, Henrik W.K., p.15

[180] Id.

Still CCC involves at least two innovations compared to the previous state of things. First improvement is on collection of evidence and trans-border search in article 32. According to the provision, parties *may, without the authorization of another Party* can 1- access and download any open source computer data and 2- access or receive stored computer data located in another Party, if that Party has the consent of the person who has the lawful authority to disclose that data.[182]

The second feat CCC accomplishes is that even though article 22 does not include an obligation to prosecute or investigate, as Kaspersen points out, it *"contributes to customary international law by obliging its Parties to establish jurisdiction over the offences defined in the Convention, the obligation in Article 22 may have a wider impact than only cybercrimes."*[183]

While these changes effectively reduce the possibility of a negative jurisdictional conflict and mitigate the troubles of acquiring cross-border evidence, they also require states to develop higher levels of international cooperation and acquire authority to perform previously unlawful acts. We do not know if Kaspersen was actually expecting to see similar provisions in other international agreements but the same approach can also be found in the infamous Anti-Counterfeiting Trade Agreement –only this time stronger.

2. Effects of ACTA to Jurisdiction in Cyberspace

In spite of the major effort by the parties to keep the negotiations secret, the 'Wikileaks' incident revealed that several governments have been working on an international agreement

---

[181] Id.

[182] Art. 32 CCC

[183] Koops & Brenner; 'Cybercrime and Jurisdiction', p. 21

regarding the protection of intellectual property right called Anti-Counterfeiting Trade Agreement or ACTA.[184]

According to the preamble, main aim of ACTA is to *"address the problem of infringement of intellectual property rights, including that which takes place in the digital environment, and with respect to copyright or related rights in particular in a manner that balances the rights and interests of the relevant right holders, service providers and users"*[185] The reason of the widespread protest and massive criticism that confronted ACTA was the alleged absence of such balance in the provisions; yet we will only discuss parts of the agreement that are relevant to our subject.

The criminal law aspect of the agreement is based on the crime definitions in Article 23 of the Agreement. This article obliges Parties to criminalize *"willful trademark counterfeiting or copyright or related rights piracy on a commercial scale"*[186] and *"willful importation and domestic use, in the course of trade and on a commercial scale, of labels and packaging."*[187] Then under Section 5 of the same chapter, entitled 'Enforcement of Intellectual Property Rights in the Digital Environment', it is specified that parties have to implement necessary laws to ensure legal action can be taken against infringements that take place in digital environment.[188] Criminal copyright infringement is without doubt a cybercrime in the general sense; or more specifically a content crime.[189] These two provisions confirm that ACTA, even though its title or

[184] Wikipedia article on ACTA <http://en.wikipedia.org/wiki/Anti-Counterfeiting_Trade_Agreement>

[185] ACTA, *Anti-Counterfeiting Trade Agreement*, Preamble

[186] Art. 23 (1), Chapter 2 Section 4; ACTA, *Anti-Counterfeiting Trade Agreement*

[187] Art. 23 (2), Chapter 2 Section 4; ACTA, *Anti-Counterfeiting Trade Agreement*

[188] Art. 27 (1) and (2), Chapter 2 Section 5; ACTA, *Anti-Counterfeiting Trade Agreement*

[189] Walden, Ian; p.23

preamble does not suggest, is an agreement that, along with other things, regulates criminal conduct in cyberspace.

Furthermore, again under section 5, it is stated that, *"A Party may provide…its competent authorities with the authority to order an online service provider to disclose expeditiously to a right holder information sufficient to identify a subscriber whose account was allegedly used for infringement…".*[190] Due to the vagueness of the term "allegedly used for infringement', this provision effectively allows signatory states to gain total access to the data stored by ISPs. Finally, with the aid of Articles 33 and 34, entitled 'International Cooperation' and 'Information Sharing' respectively, the Agreement also enables and promotes the flaw of this information among signatory states.

This procedural regime illustrated here is clearly an improvement over the limitations of Article 32 of CCC. In fact, the level of international cooperation aimed in ACTA is far surpassing CCC. If the provisions in ACTA were to be enforced to full extent, movement of information and evidence for cybercrime would probably improve significantly. In such a scenario we can also expect changes in jurisdictional approaches as a consequence to the mitigation of difficulties in cross-border prosecutions. Undoubtedly, this improvement would be at the cost of restrictions on individual liberties and sovereignty of states; which lead us to question the merits of international cooperation.

[190] Art. 27 (4), Chapter 2 Section 5; ACTA, *Anti-Counterfeiting Trade Agreement*

3. International Cooperation and The Future of Cybercrime Jurisdiction

Gus Hosein, pointing at the inclinations of jurisdiction theories, wrote that: *"…we have allowed jurisdiction to become only a legal issue. In time we have forgotten that jurisdiction is also a highly political concept. We need to recall that power and sovereignty are integral ingredients to our understanding of jurisdiction."*[191] Parallel with the remarks of Hosein, throughout the thesis we have referred to the sovereignty element in jurisdiction multiple times as we also believe any compromise in jurisdiction is in fact compromising from sovereignty. After examining the trends in jurisdiction theories in Europe and North America and promotion of international cooperation in CCC and ACTA, it is clear now, that rigid nature of sovereignty is softening.

Whereas the legal doctrine discusses solutions to solve jurisdictional conflicts in general, states are effectively unifying their jurisdictional powers more and more to the extent that there will be no conflict but an amalgamated mechanism of criminal jurisdiction. If ACTA gets into force it would not be surprising to see similar international agreements that further enhances international cooperation in criminal prosecutions and criminalizes certain behavior internationally. The question we have to ask is: Does this "merging criminal jurisdiction through cooperation" approach benefit the public?

Without doubt, increase in cooperation brings an increase in surveillance and profiling too; the provisions in ACTA regarding ISPs are a perfect example of this. Furthermore, this phenomenon increases the likelihood of individuals to face criminal prosecutions initiated by foreign states. Rousseau's social contract suggests that, normally, public transfers its right to punish to state and state uses that power to make criminal laws and punish those who offend

these laws. While we acknowledge the purpose and necessity of extraterritorial jurisdiction theories, we also notice that their 'exception' status is being corroded. Consequently, some fundamental rights of the individuals are being restricted.

Conclusion

Back in the first chapter our initial observations regarding the problem with cybercrime jurisdiction was as follows:

1- *The state(s) that can and should claim jurisdiction may not exercise its power.*

2- *A state that should not have asserted jurisdiction may do so based on a fictitious link and start prosecution.*

The first premise appeared as a problem that is caused by lack of adequate legislation, expertise, technical capacity or simply lack of will to prosecute and the latter as a result of the expansive approach that predominates jurisdictional theories.

Therefore we decided to analyse all known jurisdictional theories from a cybercrime perspective to determine which of these may help us in regard to these two premises above.

In the end, the case law and national laws from the countries we have chosen revealed us that, the second premise is more of a concern; since not only that the application field of territoriality principle is expanded but also extraterritorial theories are used more often; which considerably lowers the chance of the first premise coming true.

---

[191] Koops & Brenner; 'Cybercrime and Jurisdiction', p. 23

However we also realised that some of these jurisdictional theories appears to be intrinsically incompatible for certain types of cybercrime due to their unusual characteristics. Specifically, we noticed that:

- Even though the territoriality principle is the most fundamental of all jurisdiction principles, because of the way it is construed, it enables states with a very remote connection to a cybercrime to assert jurisdiction and prosecute. Content crimes and virus attacks are prime examples of this.

- Especially, applying objective territoriality and other similar expansive theories to content crimes appeared to be highly controversial and even against some fundamental principles of criminal law. For this reason we suggested the approach found in the German legal doctrine, which distinguishes uploading data from downloading data in regard to content crimes. This approach basically suggests that, just because a website is accessible in a state's territory, that state shall not exercise jurisdiction over its contents; unless the data is not 'pushed into' the computer systems located within the state's territory via e-mail or similar methods. On the other hand we also acknowledged that it is inside the limits of a state's sovereignty to regulate or restrict contents of domestic websites and we agreed with the possibility of a website to be located on a server in country X while targeting nationals of country Y and exploiting this situation.

  Therefore, the territorial approach we suggest for content crimes is to accept the law of the server's country as long as: **1)** the content data is **not pushed into** the computer system located in another country **2)** the content is **not specifically targeting** viewers located in another country and creates a **substantial negative effect** in there.

- Extraterritorial theories show different levels of compatibility with cybercrime. **Passive nationality** may create jurisdictional problems in the event of crimes with large amounts of alleged victims; such as content crimes with victims or virus attacks. For content crimes, we believe the intended target of the crime might also be checked here for better results. Nevertheless, as long as the claim is limited with double criminality principle like in Germany and UK laws, it is a solid theory to assert cybercrime jurisdiction. **Active nationality** theory is considered to be the second most important of jurisdictional theories after territoriality and also has been incorporated to CCC. We agree with the role of active nationality theory in cybercrime jurisdiction and believe that except for DDOS attacks, invoking active nationality should lead to no controversy. On the other hand, **Protective Principle**, by definition, should be saved only for very significant crimes that actually threaten a state's national security or general interests. In the case of cybercrime such a situation may occur due to military or economic espionage or a cyber-assault on country's vital systems such as power grid or transportation. That aside, invoking protective principle is not appropriate and might be considered illegitimate. **Universality Principle** is the most problematic of all theories due to the level of consensus on the nature of cybercrime. While believe, for many types of cybercrime, it is still early to claim that they are *"recognized by the community of nations as of universal concern."*[192]

- Even when we apply the theories properly, as a result of the nature of cybercrime, most likely, there will be multiple jurisdictional claims regarding the same criminal conduct and consequently it will be difficult to avoid positive conflicts of jurisdiction. In order to solve

[192] Restatement § 404

these conflicts and give priority to one of the states, we analysed numerous factors we could find in national laws, bilateral agreements and legal doctrine.

- Among these factors we examined, some appeared to be more effective at ensuring the state with strongest claim receives the priority in regard to cybercrime. We do not aim to provide a precise ranking of these factors since we think that the importance of factors may change from case to case. However we can still distinguish some of the factors that usually have a greater weight than those with a lesser impact.
- With our evaluation **primary factors** that should be considered in a jurisdictional conflict regarding cybercrime are: **harm**, **nationality of the offender, character of the crime, importance of the regulation to the regulating state, importance of the regulation to the international system** and **consistency of the regulation with other states regulating such activities**.
- On the other hand, we saw that multilateral agreements regarding the subject have assumed a completely different approach to the problems we have been discussing so far. Both CCC and ACTA, instead of providing legal guidance on these concerns many scholars in the legal doctrine share, focus on enhancing international cooperation, information sharing and cross-border searches; eventually aiming to restrict the limits of sovereignty of the individual state.

The bigger picture here is that states are altering the understanding of jurisdiction with the help of multilateral agreements and do not refrain from restricting the rights of the individual while doing so. In this system, the content of sovereignty is shrinking in size. We believe this phenomenon is similar to people renouncing their natural right to punish wrongdoings and transfer that right to the state so that the state becomes the sovereign punisher; only this time

states are renouncing their right to punish wrongdoings in their territory and transferring it to an amalgamation of sovereignty. This may have started from cybercrime jurisdiction but as Sieber guessed it will probably continue with other types of crime in time.

BIBLIOGRAPHY

BOOKS

Clarke, Richard A. and Knake, Robert K.; *Cyber War*, HarperCollins Publishers, 2010.

Koops, Bert-Jaap and Brenner, Susan W.; *Cybercrime and Jurisdiction – A Global Survey,* TMC Asser Press, 2006.

Walden, Ian; *Computer Crimes and Digital Investigations*, Oxford University Press, 2007.

Wall, David S., *Crime and Deviance in Cyberspace*, Ashgate Publishing, 2009.

Wall, David S.; *'Cybercrime- The Transformation of Crime in the Information Age'* , Polity Press, 2011.

ARTICLES

Goodman, Marc D.; Brenner, Susan W.; '*The Emerging Consensus on Criminal Conduct in Cyberspace'*, 2002, available at:<http://ia600406.us.archive.org/18/items/TheEmergingConsensusOnCriminalConductInCyberspace/TheEmergingConsensusOnCriminalConductInCyberspace.pdf>.

Johnson, David R.; Post, David G.; *'Law and Borders – The Rise of Law in Cyberspace'*, Stanford Law Review Vol:48, 1996, available at: < http://cyber.law.harvard.edu/is02/readings/johnson-post.html>.

Menthe, Darrel; *'Jurisdiction in Cyberspace: A Theory of International Spaces'*, MICH. TELECOMM. TECH. L. REV. 69, 1998, available at: <http://www.mttlr.org/volfour/menthe_art.html>.

Brenner, Susan W.; Koops, Bert-Jaap; '*Approaches to Cybercrime Jurisdiction'*, Journal of High Technology Law 2004. available at: < http://papers.ssrn.com/sol3/papers.cfm?abstract_id=786507>.

Wolswijk, H.D.; *'Locus Delicti and Criminal Jurisdiction'*, Netherlands International Law Review, XLVI; 1999.

REPORTS, OFFICIAL DOCUMENTS

Kaspersen, Henrik W.K., Council of Europe Report Draft, *"Cybercrime and Internet Jurisdiction"*, 2009, available at: < http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/T-CY/2079_rep_Internet_Jurisdiction_rik1a%20_Mar09.pdf>.

Committee of Experts on Crime in Cyber-Space, Explanatory Report on Convention on Cybercrime, 2001. available at: <http://dasalte.ccc.de/cybercrime/mirror/FinalCyberRapex.htm>.

Princeton Project on Universal Jurisdiction, *The Princeton Principles on Universal Jurisdiction*, 2001, available at: <http://www1.umn.edu/humanrts/instree/princeton.html>.

Eurojust Annual Report 2003, 'Guidelines for deciding "which jurisdiction should prosecute?" available at <http://www.eurojust.eu.int> .

WEBSITES

Oxford Dictionaries Online; http://oxforddictionaries.com/

PC World News; http://www.pcworld.com

Proskauer Guide; http://www.proskauerguide.com

German Law; http://www.gesetze-im-internet.de