Ignorantia Terrae Non Excusat

A discussion paper regarding the locality of enforcement

for the

Crossing Borders: Jurisdiction in Cyberspace conference - March 2016

M. Zoetekouw (LL.M)

Introduction

Ignorantia juris non excusat is a maxim that has found a place in many domestic legal systems in one form or another. It expects all citizens to know the law, or at the very least, denies them the possibility to claim ignorance of the law as a defence to its breach. One may safely expect, assuming the existence of a rule of law, that if such a rule is leveraged against an average citizen it would certainly be true - and probably more so - for trained law (enforcement) professionals.

This paper will deal with the assumption with regard to enforcement in cyberspace

> ***if one cannot determine the physical nexus to one's 'position' in cyberspace one may assume to be operating within one's own territory and therefore has jurisdiction.***

The 'one' referred to above is usually an operative of law enforcement or the prosecution office. This begs the question that if we preclude the average citizen from claiming a lack of knowledge of the law as an excuse, why would we allow trained specialists such a claim. In this case the claim would not be so much about ignorance of the law, but ignorance of *applicable* law, because applicable law is determined through territory and the locality cannot be determined. Differently put: There is no loss of (physical) location in cyberspace, only loss of knowledge of that location[1] and with that the law that governs that location. Not knowing the location then becomes an indirect way of claiming ignorance of the law, while trained law specialists ought to be held to at least the same standard as ordinary citizens, arguably a higher one.

This paper recognises that there is a problem that needs to be solved with regards to enforcement in cyberspace, but will question whether the solution should be found in creating a fiction of territoriality based on the difficulty of finding a physical nexus to which to tie one's jurisdictional claims.

To this end this paper will deal with enforcement (measures) in cyberspace based on jurisdictional claims of territoriality. It will start by asserting that we do indeed have a problem with law enforcement in cyberspace that needs to be solved. Next it will, very briefly, touch upon some basic concepts of international law that are part of any kind of discourse regarding law enforcement in cyberspace. The paper will then turn to enforcement jurisdiction in cyberspace, limited to claims of territorial jurisdiction. The paper will then address the assumption outlined above and move on to conclusions about its tenability.

Disclosure and asserting the problem

Besides working as a Ph.D. researcher within the UNIJURIS project at Utrecht University I hold a position as Legal Advisor on matters of Cybercrime & Digital Technology to the Dutch Police.[2] It is a job

[1] Koops, B and Goodwin, M, Cyberspace, the cloud and cross-border criminal investigation – the limits and possibilities of international law, Tilburg university, TILT, december 2014 p 12, 48

[2] I expressly state here that the complete content of this paper represents my professional legal opinion as an academic alone. In no case can any position in this paper be assumed to be that of the Dutch National Police, nor has the Dutch National Police had any say or influence in the content or wording of this paper whatsoever.

which I've held for nearly 10 years now, during which time I have seen cybercrime grow from a phenomenon on the societal fringe to one in the full spotlight of public attention. This is true not only for the Netherlands, but for many countries in the process of digitalisation and globalisation. During this time I have witnessed - and advised in - numerous cases and have taken part in discussions, policy- and law-making sessions regarding regulation of and law enforcement on the internet.

In the 1990's the focus of the nascent cyberlaw was primarily on norms and behavioural regulation. States needed to figure out how to adapt old concepts to new crimes or new methods of committing crimes. While the process is never complete, attention did shift to procedural law in the late 1990's and early 2000's. Old powers of investigation seemed limited or ill-suited to combat crime with cyber-components or made it outright impossible driving early adapters to make accommodations for 'digital policing' in their law systems. We have now arrived at a point at which many countries have developed both normative and procedural laws dealing with the 'cyber' environment. They may have either acceded to with the Budapest Convention[3] and implemented its requirements within national law, taken it as an example without actually signing up or have developed a set of rules to deal with 'cyber' completely independent of these developments.

While law and law enforcement have -slowly- adapted both with regards to the norms as well as (criminal) procedure to handle investigations of 'cyber' crime, neither of them seems to be able to keep up with technical developments and the corresponding societal and law enforcement needs. One important field where law enforcement needs are outpaced by developments in society is mutual legal assistance (MLA). Cyberspace enables a wide geographical spread of evidence, proceeds, victims and involved suspects requiring a state seeking enforcement to make extensive use of MLA's. MLA is in most cases based on bi- or multilateral treaties. Fact is however, that not all countries have MLA relationships, whether treaty-based or not. With cyberspace essentially connecting all countries as virtual neighbours, shortening the time to 'move' halfway across the globe to less than it takes to get to the local supermarket, this is a problem for law enforcement. Even when a proper MLA relationship is in place these procedures are usually accompanied by many administrative, procedural and organisational safeguards that are needed to approve or pass on the content of a request for aid. One of the characteristics of this process is that it is, in many cases regrettably and in some cases insurmountably, slow. This is particularly true of the area of cybercrime, where speed is even more essential to law enforcement than for other types of crime. While MLAT's[4] in general and the Budapest Convention[5] in particular aim to remove barriers and streamline requests, in the latter case through for instance 24/7 contact points, it is in many cases simply not sufficiently fast to be effective when all the rules are adhered to.[6] By the time MLA's are executed, proof, profit or persons have long gone. Since even this point is a subject of debate I will spend a few paragraphs on this issue before moving on.

Denying the problem

It is regularly called into question - or even outright denied – by commentators ranging from politicians and policy workers to IT-industry representatives to academics as to whether the slowness of MLA procedures, or the lack of (use of) them, is indeed a problem.[7] They are quick to assert that there have been dramatic increases in the number of investigations and prosecutions of so-called cyber cases in recent years. Commentators have also pointed to a dearth of quantitative evidence to suggest that mutual legal assistance has failed in such instances, alongside a lack of official protest when it does. This call for number and statistics is also increasingly heard in (semi-)legal circles. Not quite as much attention is granted to the reasons why there may be a(n) (significant) amount of underreporting of issues as well as alternative reasons for not wanting change the current MLA system.

Undenying the problem

As a law practitioner[8] I am ill-equipped to deal with matters of numbers and statistics. It is not part of our normal curriculum and rare is the fine legal mind that has chosen law for his studies and profession because of their excellence in mathematics related topics. However, one conclusion I dare draw is that the absence of numbers on failures does not mean absence of failure. A simple question clarifies this statement: Why would law enforcement professionals, politicians or anyone else painstakingly report failures to gain information necessary to advance an investigation absent a legal duty to do so? Besides *possibly* showcasing a need for better

[3] Convention on Cybercrime – Treaty no. 185, Council of Europe, Budapest 23-11-2001
[4] Mutual Legal Assistance Treaties
[5] see note 3
[6] In many (advanced) cybercrime cases when an opportunity for enforcement does present itself or is brought about the window of opportunity for taking action usually ranges from a few hours to a few days. MLA procedures usually take several days in a best case scenario. Outside such a scenario time-to-execution may range from a few weeks to many months, at which time their execution is often no longer relevant.
For reference: Fidler, Mailin, MLAT Reform: Some Thoughts from Civil Society; https://www.lawfareblog.com/mlat-reform-some-thoughts-civil-society
[7] An example of the last: S. Carrera et all, Access to Electronic Data by Third-country law enforcement authorities, Centre for European Policy Studies, 2015, p 65-74
[8] of (dutch) criminal and international law

or faster MLA that someone *might* address, it *certainly* would show a weakness against actions deliberately taken to hinder law enforcement efforts.[9] Many a good reason exists not to put this problem front and centre in the public eye. Law enforcement wants no unsolved cases on their records; politicians do not want to have to explain why they are unable to give law enforcement the tools they need and states have interests in continued good relations that might be damaged by pointing fingers - just to name a few obvious factors.

I certainly have no better quantitative evidence of the failures of the MLA system then others have for their claims of success. What I do have is an inside view and more than one or two stories as to how cases with a cybercomponent fail to be resolved or even commenced due to the (perceived) slowness of MLA requests. These cases are aborted or never even started due to the (perceived or real) lack of opportunities to gather necessary evidence in an efficient or even just a timely manner. This view is supported by statements from government, academia[10] , interest groups, the IT industry[11] as well as results of the work by the (now renamed) Transborder Group[12] of the Cybercrime Convention Committee[13] and the UNODC[14] based on (member-)state polling as well as more qualitative methods.

Approached from a different angle: Why would we be seeing states advancing all kinds of 'solutions´[15] to this problem if the existing MLA circuits were proving to be effective, considering the fact that alternatives are all more or less legally tenuous and/or politically charged?

International law and relations are anything but numbers-based; many other factors tend to weigh just as much or even more heavy than the quantifiable aspects. So relying (purely) on those aspects to try to prove or disprove a problem is, in a word, nonsensical.

As a departure point for the rest of this paper I will state that lack of enforcement is a problem in cyberspace is a problem. One that will not easily be fixed for the two major reasons described above: the lack of all-encompassing MLA relationships and slowness of MLA when such a relationship does exist. Before turning to discussing enforcement in cyberspace on the basis of claims of territoriality, a very condensed overview of some basic concepts will first be given. Only then it will focus on the question as to whether one may indeed assume jurisdiction through territoriality without a physical nexus.

Brief overview of concepts of Territory, Sovereignty, Jurisdiction

If one looks at cyberspace and wishes to discuss the deployment of enforcement jurisdiction there one is hard pressed to avoid talking about general concept like sovereignty and territory, since those two are closely tied together and also to the notion of jurisdiction. Since these concepts are interlinked it will be impossible to avoid some referencing back and forth as they are covered. Spatial constraints dictate that this overview be brief so some generalisation and skipping of nuances is unavoidable.

Territory

The notion of territory has been of the founding pillars of the international legal order since the Peace of Westphalia[16], and is very tightly intertwined with the concepts of sovereignty and jurisdiction. The international legal order is (mostly) comprised of sovereign states. Territory is one of the, perhaps even *the,*

---

[9] There is little to be gained in publicly broadcasting what techniques to use or in what countries to store part of your cybercrime infrastructure or proceeds or methodology. At best there could be a chance that something would be done to change it. For certain it would advertise such knowledge to those of ill will that did not yet have it.

[10] Force Hill, Jonah, Problematic Alternatives: MLAT Reform for the Digital Age, Harvard Law School National Security Journal, 28-01-2015 http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/; Swire, P and Hemmings, J., Re-Engineering the Mutual Legal Assistance Treaty Process, in: NYU Annual Survey of American Law (forthcoming 2016). Draft @ http://www.heinz.cmu.edu/~acquisti/ SHB2015/Swire.docx; Goodman, Marc, International dimensions of cybercrime, In Ghosh, S and Turrinee, E. *Cybercrimes: A Multidisciplinary Analysis.* Springer, 2011. 332-334.

[11] For example: Time for an international convention on government access to data, http://blogs.microsoft.com/on-the-issues/2014/01/20/time -for-an-international-convention-on-government-access-to-data/Jan 2014; Google defends its use of data, points finger at governments, http://www. businesscloudnews.com/2015/02/16/google-defends-its-use-of-data-points-finger-at-governments/

[12] In full: Ad-hoc sub-group on Jurisdiction and Transborder access to data and data flows.
Ad-hoc subgroup on Transborder Access and Jurisdiction, report: Transborder access to data and jurisdiction: Options for further actions by the T-CY, T-CY (2014)16, Council of Europe, 03-12-2014, p 8, 10, 12

[13] See note 10 as well as Cybercrime Convention Committe, The mutual legal assistance provisions of the Budapest Convention on Cybercrime - CY(2013)17rev (Provisional), Strassbourg 2014, p 3, 123-124, more details in state responses

[14] see United nations Office on Drugs and Crime, comprehensive study on Cybercrime - draft, UN, 2013, p 169, 183,

[15] To just point out a few: extensive extraterritorial territorialification by civil law countries, Belgiums law for remote search and seizures (88ter wetboek van strafvordering), and the 'uncertain location' claims of the up and coming CCIII law in the Netherlands, Kamerstukken II, 34372, 3 – memorie van toelichting, p 11, 33, 45-50 https://zoek.officielebekendmakingen.nl/kst-34372-3.pdf

[16] Or at least since the times of Vattel. De Vattel, E., 1793. The Law of Nations; See also Beaulac, S., 2003. Emer de Vattel and the Externalization of Sovereignty. Journal of the History of International Law, 5(2), pp.237-292.

most basic requirements of statehood. When one is not a state, one cannot claim sovereignty. When one cannot claim sovereignty, one cannot claim powers of jurisdiction anywhere, nor would one have the right to do so. While land may exist without sovereignty, without the presence of a controlling sovereign land is not territory, but is merely land.[17] However one approaches the topic, in this tangle of cross-referencing concepts territory plays an important role.

As a sovereign one is (or ought to be) in control over a territory and anything or anybody in that territory falls under ones jurisdiction.[18] This sovereign control of territory is tangible in many aspects easily observed in the physical world.[19] Since territory is a defining aspect of being a sovereign state as well as the defined area in which state has absolute authority and 'full control', it follows that when claiming jurisdiction, territorial jurisdiction is the strongest possible claim one can make.

Sovereignty

While a unified definition of exactly what sovereignty is does not seem to exist[20], by and large it is agreed upon that sovereignty is the position of utmost authority one can claim. A sovereign therefore knows no higher authority and requires no-one's permission to do as it sees fit within its own territory.[21] Sovereignty is self-referential and by definition exclusive and absolute (even in modern times, at least as a starting point).[22] Sovereignty, through a long history of international law, is only awarded to states.[23] Statehood and sovereignty are closely related concepts that reinforce each other's existence. One cannot be a sovereign without being a state, ones statehood is in serious doubt when a state is unable to express it's sovereignty.[24]

Sovereignty is marked by a positive and a negative aspect. The positive aspect is a sovereign's right to shape its internal order according to its own wishes, a large part of which is done through the claiming and the expression of jurisdiction. This expression of jurisdiction is all it's forms, prescriptive, enforcement and adjudicative, is both dependent on and proof of sovereignty. The negative aspect is the mirror image of the positive one, the right to non-intervention. The principle of non-intervention forbids sovereign states from meddling in each other's internal order,[25] thus allowing each the freedom to shape their own internal order.

Jurisdiction

For this paper it will be assumed the reader is aware of standard doctrine and literature regarding jurisdiction as the limited length of this paper does not allow for fuller detail.[26] As it is not necessary for this paper I will almost entirely skip prescriptive and adjudicative jurisdiction (though it is recognised that enforcement jurisdiction cannot exist without prescriptive jurisdiction) and only affirm that nations are indeed (largely) free to make the rules they wish even concerning acts that (partly) happen abroad and that they have a general right to back up these rules through adjudication of those who ignore them.

Doctrine, as confirmed in the Lotus case,[27] indicates that as a matter of principle when and how

---

[17] For reference: Island of Las Palmas case, Permanent Court of Arbitration, 1928, p 838

[18] See note 17 and Buxbaum, H.L. Territory, Territoriality, and the Resolution of Jurisdictional Conflict, American Journal of Comparative Law, 2009 p 631, 632

[19] There are maps, descriptive treaties, border patrols, name signs, presence of enforcement personnel in national uniforms etc.

[20] Crawford, J. The Creation of States in International Law (2nd Ed), Oxford University Press, 2007

[21] See note 17

[22] Even through Vatellian absolute sovereignty does not truly exist anymore in modern times are states are bound by resolutions of the United Nations General Assembly and (limiting) rules of (customary) international law. See Shaw, M.N. International law (7th ed), Cambridge University Press, 2014, p 471, see also Tsagourias, N, The legal status of Cyberspace, in: Tasgourias, N and Buchnan, R. Research Handbook on International Law & Cyberspace, p 17, Edward Elgar Publishing, 2015

[23] Although some publications and 'trends' exist that point to a future where this may not necessarily be true anymore See for instance: Brauer, J and Haywood R, Non-state Sovereign Entrepreneurs and Non-territorial Sovereign Organizations, working paper NO 2010/09, United Nations University; Weir, J.P>, Sovereign Citizens: A reasoned response to the madness; Taylor, C.R, A Modest Proposal: Statehood and Sovereignty in a
Global Age, Journal of International Law, 2014, p. 745-809

[24] Crawford, J. The Creation of States in International Law (2nd Ed), Oxford University Press, 2007; Lapidoth, R. When is an Entity entitled to statehood?, Israel Journal of Foreign Affairs, 2012 p. 77-81

[25] See UN charter, art. 2(7); the Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States, annex to GA resolution A/RES/20/2131 (XX), 21 December 1965. Please also refer to the Corfu Channel case, ICJ Reports 1949, 35, the Military and Paramilitary Activities case, ICJ Reports 1986, 202, and the Nicaragua case, ICJ Reports 1986, 14, 109-10. See also Shaw, M.N. International law (7th ed), Cambridge University Press, 2014, p 471

[26] For reference see Michael Akehurst, "Jurisdiction in International Law" (1972-73) 46 Brit. Yb. Int'l L. 145, and Shaw, M.N. International law (7th ed), Cambridge University Press, 2014, p 469-505

[27] S.S. "LOTUS" PCIJ Series A no 10, ICGJ 248 (PCIJ 1927), 07-09-1927 par. 46 & 47 "It does not, however, follow that international law prohibits a State from exercising jurisdiction in its own territory, in respect of any case which relates to acts which have taken place abroad, and in which it cannot rely on some permissive rule of international law. Such a view would only be tenable if international law contained a general prohibition to States to extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, and if, as an exception to this general prohibition, it allowed States to do so in certain specific cases. But this is certainly not the case under international law as it stands at present. Far from laying down a general prohibition to the effect that States may not extend the application of their laws and the jurisdiction of their courts to persons, property and acts outside their territory, it leaves them in this respect a wide measure of discretion, which is only limited in certain cases by prohibitive rules; […] In these circumstances all that can be required of a State is that it should not overstep the limits which international law places upon its jurisdiction; within these limits, its title to exercise jurisdiction rests in its sovereignty."

jurisdiction in general is asserted is completely up to the wishes of the sovereign state[28] and on the basis of principles of that state's choosing. As long as this claim is compliant with the states internal order this is lawful and cannot be called into (legal) question. A state wishing to claim jurisdiction requires permission of no-one nor a permissive principle of international law. While this part of the decision in the Lotus case has faced considerable doctrinal criticism as being too lenient, until today has not been overturned and remains *the* leading case with regards to jurisdiction in international law. For now, until the matter is revisited, Lotus remains the starting point for any discourse with regards to claiming jurisdiction.[29] That said, developments after[30] the Lotus case as well as state practice do seem to indicate that states require claims of jurisdiction to be founded on a permissive principle with at least a legitimate interest in hand.[31]

Enforcement Jurisdiction

Like sovereignty, enforcement jurisdiction does not seem to have a general agreed upon definition. For the remainder of this paper 'enforcement jurisdiction' is used to mean organs of state leveraging powers of investigation and using coercive measures against persons and items needed to investigate criminal acts.[32] The measures needed to enforce judicial decisions are excluded from this definition.

In the case of enforcement jurisdiction specifically, things are a little different, indeed clearer, than for jurisdiction in general. The freedom to assert jurisdiction as one sees fit noted above is, with regards to enforcement jurisdiction, only true when these enforcement measures are used *within* the territory of the enforcing state, where its authority is absolute. Once operating outside of its territory, the state loses its position of ultimate authority and has to rely on permissive rules of international law to claim jurisdiction.[33]

A state looking to enforce its laws outside it's own territory will in most cases (outside the high seas and in any remaining areas of terra nullius) be operating in another state's territory. That state too is the highest authority within its territory and fully able to determine when and how enforcement of laws may occur. Enforcing one's own laws in another's territory without that state's express permission amounts to an interference that is forbidden by the principle of non-intervention, as confirmed by the Lotus case.[34]

While the principle of non-intervention is a general principle of international law that is always valid, it especially relevant in the enforcement of criminal law. The enforcement of criminal law has traditionally been -and still is-, one of the most jealously guarded rights of a sovereign state.[35] This is not surprising as this enforcement involves deployment of state power that is, at least potentially, both highly coercive as well as laden with normative values.[36]

Deployment of enforcement measures in the jurisdiction/territory of another state certainly amounts to intervention and is, apart from of the actual use of force, one of the most invasive breaches of a state's internal sovereignty, with invasiveness only increasing as the amount of 'coercion' increases. This premise has not lost any of its strength despite the strong globalization of the last decades. Nothing much has changed in this respect since the Lotus case. Although a few examples exist of states (openly) enforcing their laws outside their territory, such actions have generally been met with resistance and protest from other states. Despite it's venerable age, this part of the Lotus verdict still stands unassailable, being very much in line with current state practice and drawing little academic criticism.[37]

Consequently the state seeking to extraterritorially enforce it's rules has no authority other than that which is granted to it by the state where the enforcement is to take place.[38]

---

[28] Some limitations based on treaties and international law do exist in modern times, but this does not invalidate the principle as a starting point

[29] See also: Kohl, U., Jurisdiction in Cyberspace, in: Tasgourias, N and Buchnan, R. Reseearch Handbook on Internationnal Law & Cyberspace, p 51, Edward Elgar Publishing, 2015

[30] See the"Harvard Draft": Draft Convention on Jurisdiction with Respect to Crime, The American Journal of International Law, 1935 439-442

[31] Ryngaert, C.M.J., Jurisdiction in International Law (2nded) , Oxford University Press, 2015, p 38- 40

[32] Cmp. V. Lowe, "Jurisdiction" in M. Evans, ed., International Law (Oxford: Oxford University Press, 2003), p 329.

[33] Ryngaert, C.M.J, Jurisdiction in International Law (2nded) , Oxford University Press, 2015 p 9

[34] Brownlie, Principles of international Law. 4th edition p 310 and S.S. "LOTUS" PCIJ Series A no 10, ICGJ 248 (PCIJ 1927), 07-09-1927 par 45 "Now the first and foremost restriction imposed by international law upon a State is that – failing the existence of a permissive rule to the contrary – it may not exercise its power in any form in the territory of another State. In this sense jurisdiction is certainly territorial; it cannot be exercised by a State outside its territory except by virtue of a permissive rule derived from international custom or from a convention." See also Stigall, D.E, Ungoverned Spaces, Transnational Crime, and the Prohibition on extraterritorial enforcement jurisdiction in international law, Notre Dame Journal of International & Comparative Law, 2013, 9

[35] Henkin, Louis, Humand Rights and State "Sovereignty", Georgia Journal of International and Comparative Law, 1995 p 31-45

[36] Stigall, D.E, Ungoverned Spaces, Transnational Crime, and the Prohibition on extraterritorial enforcement jurisdiction in international law, Notre Dame Journal of International & Comparative Law, 2013, 10

[37] Koops, B and Goodwin, M, Cyberspace, the cloud and cross-border criminal investigation – the limits and possibilities of international law, Tilburg university, TILT, december 2014 p 8

[38] V. Lowe, "Jurisdiction" in M. Evans, ed., International Law (Oxford: Oxford University Press, 2003), p 184

Enforcement (Jurisdiction) in Cyberspace

In the previous section of this paper we saw that jurisdiction based on territory is considered the strongest claim one can make. Where enforcement jurisdiction is concerned this is even more so the case as it is the only principle by which a state does not have to rely on the cooperation or consent of another state. Territoriality remains the defacto standard of enforcement effort.

However, while we habitually refer to cyberspace as a place, one cannot actually 'go there'. Cyberspace as such does not exist in the physical world; It is an imaginary construct of the human mind and the technology we used to create it.[39] In and of itself it is completely a-territorial. Any territorialisation one might want to assign to it accordingly needs to be constructed.

When traversing the internet for normal purposes hints for a territorial nexus can be found in several ways. One may look at the language of communication (though for a large part of the internet the lingua franca is English and therefore holds no special meaning), or look at the top level domain[40] where a website, forum or service is registered or try and trace the ip-adress that goes with it. While such methods certainly give clues, none give certainty.

The physical location of the data or process is becoming of increasingly little consequence in cyberspace, not just 'socially' but also technically. Data is moved around by algorithms without human intervention, sometimes without the possibility of human intervention. This makes no difference to the user as long as he can access his data, but it does matter when one is trying to ascertain a territorial nexus.

Technical developments have also brought about that 'a document' or file or even a 'running process' no longer need to be in one place anymore. It may be cut up in a thousand pieces and dispersed over as many computers in dozens of countries, with the user either remaining blissfully ignorant of that fact or, in the case of a capable cybercriminal, enjoying the deliberately sought benefits of that.[41] This is already true for ´normal´ internet use, but far more so when a criminal is deliberately trying to hide the location of his person, data and infrastructure. In many cases the physical 'location' of a machine or data can simply not be divined or cannot be divined without actions that in most cases would likely constitute criminal acts in and off themselves. With this in mind, perhaps territoriality is not the right way to go about determining who has the right to enforce in cyberspace?

Non-territorial[42] enforcement in cyberspace?

With jurisdiction, territory and cyberspace remaining unwilling partners in the case of enforcement, but the need for enforcement undeniable, a point could be made for trying to move away the continuous attempts towards the (conceptual) territorialisation of cyberspace.[43] Attempts to do so include a line of reasoning that posits that enforcement in cyberspace cannot amount to a breach of sovereignty. The idea behind this is that since cyberspace is neither physical nor territorial, law enforcement activities or persons in cyberspace never actually do enter another state's territory and therefore by definition cannot breach it's sovereignty. With extraterritoriality out of the way states would then, if one follows the classic Lotus line, be free once more to shape their enforcement according to the rules of their internal legal order.

Proponents of this line of reasoning usually refer to a more philosophical discourse about the nature of cyberspace, the metaphors we use to describe it and the consequences of their use that has seen considerable academic activity.[44] Koops and Goodwin for instance[45] recently posited that enforcement activity can be likened more to 'sending a message' then 'going there' and warned us (justly) about the influence the metaphor we choose may have on our thinking. While I fully support the warning, I disagree with the 'sending-a-message'

---

[39] Cohen, J.E., Cyberspace As/And Space, Columbia Law Review, 2007, p 210-256 Koops, B and Goodwin, M, Cyberspace, the cloud and cross-border criminal investigation – the limits and possibilities of international law, Tilburg university, TILT, december 2014 p 31, 32; John Perry Barlow, A Declaration of the Independence of Cyberspace, Feb. 8, 1996, https://www.eff.org/cyberspace-independence

[40] https://www.icann.org/resources/pages/about-e5-2012-02-25-en

[41] For reference: Meijer, R.J. and Zoetekouw, M. Technical and Legal Challenges of Criminal Law Enforcement in the Digital Age, Octopus Conference 2015 https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680306450

[42] As opposed to extra-territorial

[43] See also Svantesson, D.J.B., A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, Ajil Unbound 2015, 69-74

[44] For reference: Cohen, J.E., Cyberspace As/And Space, Columbia Law Review, 2007, p 210-256; Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Cal. L. Rev. 439, 469–75 (2003); Dan L. Burk, Legal Consequences of the Cyberspatial Metaphor, in 1 Internet Research Annual: Selected Papers from the Association of Internet Researchers Conferences 2000–2002; Carrier, Michael A., and Greg Lastowka. "Against Cyberproperty." *Berkeley Technology Law Journal* 22.4 (2007): 1485-1520; Calvert, Clay. "Regulating Cyberspace: Metaphor, Rhetoric, Reality, and the Framing of Legal Options." *Hastings Comm. & Ent. LJ* 20 (1997): 541; Graham, Mark. "Geography/internet: ethereal alternate dimensions of cyberspace or grounded augmented realities?." *The Geographical Journal* , 2013, 177-182.

[45] Koops, B and Goodwin, M, Cyberspace, the cloud and cross-border criminal investigation – the limits and possibilities of international law, Tilburg university, TILT, december 2014 p 9, 12, 48-49. To be fair Koops and Goodwin do elaborate with more coercive and/or intrusive examples.

metaphor. It is as 'wrong' or even more so as the 'going there' metaphor.

One reason for this is grounded in consequences that might occur. Ddos attacks are nothing more than sending a message[46], but may cripple entire computer clusters. Law enforcement 'sending a message' **may** range from a forum post (which should in most cases be permissible) to sending a targeted malformed piece of data intended to bring down defences of a system to gain access to it's content or location or even bring down the machine outright (possibly with no regard for ancillary damage).

While 'sending a message' is more or less a technically correct way of describing what actually happens on the bits-and-bytes level, it does not properly represent what goes on at the legal level. This metaphor sounds way too innocuous for a category of activity that could potentially have the same effect as kinetic attacks. In fact, 'armed force' in cyberspace is considered sufficiently viable that in recent times its academic discussion has been far more fruitful than that concerning enforcement in cyberspace. While the approach is a little different it describes exactly this type of activity – just from a military point view.[47] Even shy of such extreme consequences law enforcement efforts could certainly inflict significant damage to or even destroy important data or computer systems, however unintended such an effect might be.

More in general I do not believe that the heart of the problem lies in the 'territorial' metaphor used for cyberspace. Consequently I do not think that replacing those metaphors with different ones will foster a satisfactory solution. The issue at the root of this problem is not whether enforcement activities physically violate the territory of another state or indeed the exact level of intrusion they commit. Rather, the issue lies with the position of the sovereign state; more specifically its sovereign right as *the* exclusive authority within its internal legal order. Put differently - the right to elaborate the level of intrusion allowed, the persons allowed to do so and the circumstances under which this is to occur are matters that, by the standards of international law, lie completely in the domain of the state in which the purported enforcement is to take place.

The very act of sending a state representative, whether virtual or physical, to create an effect in another states legal order in order to enforce the law of the sending state is a deployment of the sending states' authority into another state. This is no different in cyberspace than for any other means that could conceivably be used. When, in principle, even the simple act of merely extending an inquiry to a willing witness already[48] requires mutual legal assistance based on treaty or letters rogatory (up to the discretion of the state, it may regulate otherwise) how could enforcement activity that has a lesser degree of voluntariness or a higher degree of coercion not require the consent of the 'visited' states. By their very definition, such actions are a violation of sovereignty, no matter how well intentioned or how little 'damage' is otherwise done. Obviously, the more local effect the enforcement has, the graver the breach.

That said, such a breach is only a breach if the territorial state in question regards is at such. So if a general rule could be construed, or agreements made, in what situations such actions are deemed acceptable the problem would be mostly solved.

Extra-territorial enforcement in cyberspace

The problem of enforcement jurisdiction on the internet was recognized in the drafting process of the Cybercrime Convention[49] and serious attempts were made to incorporate rules for 'self-help' i.e. cross-border enforcement activity on the internet without requiring another's states help or permission, even if localisation within their territory was possible. Kaspersen reported[50] that, despite efforts of the drafting committee, no agreement could be reached on such far-reaching agreements and instead (a lesser) common ground was found in more efficient MLA and 24/7 contact points and article 32b of the Convention[51], which allows access

---

46 Well, actually, a lot of them – as Distributed denial of service attacks rely on overwhelming a target by sending to much 'traffic' that it is no longer able to properly respond to it, resulting in unavailability of the service for its regular users or even the complete machine going down.

47 For example: Von Heinegg, W.H., Legal Implications of Territorial Sovereignty in Cyberspace, Cyber Conflict (CYCON), 2012 4th International Conference on. IEEE, 2012; Delibasis, Dimitrios. "State Use of Force in Cyberspace for Self-Defense: A New Challenge for a New Century." interdisciplinary journal: Peace Conflict and Development 8 (2006); Roscini, Marco, Cyber operations and the use of force in international law. Oxford University Press, 2014; von Heinegg, W.H. "Territorial sovereignty and neutrality in cyberspace." International Law Studies Series, US Naval War Col. 89 (2013); Schmitt, M.N. (ed), Tallinn Manual on the international law applicable to cyberwarfare, NATO CCD COE, 2009

48 For reference: a well described overview for common procedures in English https://travel.state.gov/content/travel/en/legal-considerations/judicial/obtaining-evidence/preparation-letters-rogatory.htmlhtml (UK) Crime (International Co-operation) Act 2003, part 32; http://www.coe.int/t/dghl/standardsetting/pc-oc/PCOC_documents/PC-OC%20_2011_%2015%20%20Rev%20Consolidated%20document%20mutual%20legal%20assistance.pdf and all the deposits of national procedures by signatories to European Convention on Mutual Assistance in Criminal Matters of 1959 and in the Second Additional Protocol to that convention of 2001

49 See note 3

50 Kaspersen, W.K., Cybercrime and Internet Jurisdiction (discussion paper – draft), Council of Europe, 05-03-2009, par 79 - 89 https://rm.coe.int/ CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016803042b7

51 With transborder access beyond the situations of article 32 "neither authorised, nor precluded" the discussion of farther reaching transborder access was tabled for a later time

publicly available" on the internet without prior consent of the Convention's signatory states. Ofcourse, being a multilateral treaty, this rule is only valid for parties acceded to the convention and while successful the Cybercrime Convention is certainly not (near) global. This raises the question that if one cannot determine locality of data and with that the territorial authority how may one expect the data to be in one of the states subscribing to this agreement.

With the Cybercrime Convention into it's second decade (having drawn more signatories in that time) and the ubiquity of internet and transborder data movement at least an order of magnitude greater then at the time of it's creation the matter was revisited starting with a report[52] by the "Transborder Group" of the Cybercrime Convention Committee. Lengthy talks with many different parties ensued but by the end of 2014 it became clear that, despite the recognised needs of law enforcement, no "reasonable consensus to commence work on a [additional] Protocol [to the Cybercrime Convention]" regarding transborder access to data could be found,[53] although the Transborder Group did publish a 'common understanding' on transborder access to data in TC-Y Guidance Note #3.[54]

At the same time, outside the working of the Cybercrime Convention Committee, we have witnesses a strong move to assertions of sovereignty in cyberspace by several nations[55] also with regards to the 'use of force' through cyberspace.[56]

These developments seem to leave little room for the rule of customary international law to emerge that transborder access is indeed acceptable, even with an reported increase of countries resorting to or thinking about unilaterism despite this fact.[57]

Territorial(ized) Enforcement Jurisdiction in Cyberspace

Cyberspace so far remains thoroughly un-territorial and is becomes increasingly so as technology progresses. No amount of discussion about what metaphor to use is going to change that the international legal order as it is, is inherently territorial -a reality unlikely to change any time soon- and the basis for enforcement jurisdiction is tightly bound to that reality. Neither is progress likely to be made soon in specific instruments enabling transborder enforcement in cyberspace.

Consequently states wanting to put forward a jurisdictional claim to enforcement will have to make territorial claim. A claim that, considering the nature of cyberspace, can only be made through its territorialisation with legal fictions or proxies.[58] So, after a aside discussion of other options, we will next return to the methods used to construct territory for the purpose of enforcement in cyberspace before coming to this papers conclusion. This will include two methods quite established and one that has only recently started coming out into the light.

Territorialisation of Cyberspace

From the previous sections of this paper it should be clear that states have a considerable interest in trying to cast their enforcement activities in cyberspace as territorial. The easiest way to achieve this is to, either directly or by proxy, territorialize cyberspace itself and several methods have indeed been made to do so in the past.

---

52 Transborder Group, Cybercrime Convention Committee, Transborder access and jurisdiction, what are the options?, Council of Europe 6 december 2012 (prov), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e79e8

53 Ad-hoc subgroup on Transborder Access and Jurisdiction, report: Transborder access to data and jurisdiction: Options for further actions by the T-CY, T-CY (2014)16, Council of Europe, 03-12-2014, p 12
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf

54 Transborder Group, Cybercrime Convention Committee, T-CY Guidance Note # 3 - Transborder access to data (Article 32), Council of Europe, 09-10-2014 -
http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/Guidance_Notes/T-CY%282013%297REV_GN3_transborder_V13.pdf

55 For reference: http://thediplomat.com/2015/12/china-brings-push-for-cyber-sovereignty-to-the-un/; http://www.nytimes.com/2015/12/17/technology/china-wins-battle-with-un-over-word-in-internet-control-document.htmlacfef4d917&mc_eid=40b3c63d9b; http://thediplomat.com/2014/06/chinas-sovereign-internet/; http://www.reuters.com/article/china-cyberspace-idUSL3N14R1T120160107 ; http://www.huffingtonpost.com/lu-wei/china-cyber-sovereignty_b_6324060.html?utm_hp_ref=world; http://www.china.org.cn/government/whitepaper/node_7093508.htm

56 Schmitt, M.N.,Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013 a new version (2.0) is fortcoming with Cambridge University Press this year.

57 See note 53, p 7, 8, 13

58 For reference: Geist, M.A., Is There a There There - Toward Greater Certainty for Internet Jurisdiction, Berkeley Technology Law Journal 2001, 1345; Benoliel, Daniel, Law, Geography and Cyberspace: The Case of On-Line Territorial Privacy, Cardozo arts & entertainment law journal 2005, 125.

The Unexceptionalist Approach

The easiest way for territorialisation of cyberspace is to follow the line of reasoning of the Unexceptionalists[59] and claim that Cyberspace can be positioned territorially because cyberspace runs on infrastructure, an infrastructure that is physical and therefore can be positioned in a place, usually inside a territory. Through this infrastructure then, one may (by proxy) exert control in cyberspace.

While the Exceptionalist ideas may have lost a little of their splendour[60] the actual control of what happens in cyberspace through control of the infrastructure is limited. Even if one controls enough of the equipment to actually shut cyberspace down or make a plausible effort to monitor what goes on there, this is not the same control as being able to influence or steer all actions that happen there. As an analogy: One may 'control' a giant panda by holding it captive, or killing it. It is much harder to get it to breed, exhibit or curb aggressive behaviour or follow verbal commands. In this respect the control is fairly limited. The same is more or less true for cyberspace. In fact, as technology develops, this is becoming even more true. In the past, if one controlled (enough of) the infrastructure, one usually could get to evidence or stop a criminal act from happening or continuing. By means of true anonymization services, the move by large IT companies to full encryption to which the provider has no key[61] and several more like developments, the level of control diminishes even further.[62] While we are not (yet) at a point at which control is completely lost, the technological trend is headed in the direction of less control, not more.

Although there is usually someone to point out that (more or less) reputable companies that will cooperate with properly addressed requests from law enforcement it remains the case that control in these circumstances is limited. At the same time it is ever easier for people in the cybercrime business to avoid using those reputable services, as there are other companies, services or individuals that provide similar services who are less concerned with upholding a law abiding image.[63]

Another problem for the Unexceptionalist approach is that any cybercriminal worth his salt can and will spread his activities, data storage, and assets with the *explicit intention*[64] of spreading it over as many, preferably non-amicable jurisdictions as possible. Even if an enforcing state gets some parts of equipment or data under it's control, it will likely not have enough to complete the picture.[65]

So while the Unexceptionalist approach does solve the dogmatic legal problem it does not help in solving the enforcement problem in cyberspace and has, given the present need, outlived it's useful life.

Actual territorialisation of Cyberspace

Another way of making cyberspace (truly) territorial is by making a limited and severely gated national subsection of cyberspace. While this goes against the original ideas of it's creation[66] and poses significant technical and societal issues, it is not impossible as can be witnessed in the arrangements of China and North-Korea. If one limits cyberspace to only be available to people on one's territory and solely through machinery also located within ones territory then cyberspace has successfully been territorialized (though even that still not equates to 'full' control).

While this certainly does solve the jurisdictional issues it comes at a high cost in both a technological and a societal sense. Technological, because it requires serious reworking of the 'internet code' and infrastructure in a way opposite to the original design idea, introducing many inefficiencies. Societal because one of the greatest strengths of internet is the fast and nearly barrier-less way in which people may communicate and interact, regardless of distance, physical barriers and even cultural differences. Reshaping the

---

[59] This term refers to a academic discourse between two lines of reasoning about the applicability of state law to the internet. The unexceptionalists maintained there was nothing truly new and that everything could and should be solved with traditional rules of localisation, while the exceptionalists claimed the brave new world of cyberspace was and ought to be beyond the control of the traditional sovereign nations and therefore ought to be governed by its own laws instead of theirs. For reference: Johnson, D.R. and Post, D.G., Law And Borders: The Rise of Law in Cyberspace, 48 Stanford Law Review 1367 (1996); Goldsmith, J. and Wu, T., Who Controls the Internet?, Oxford University Press, 2006; Goldsmith, J. Against Cyberanarchy, University of Chicago Law Occasional Paper, 1999; Post, D, G., Against 'Against Cyberanarchy', Berkely Technology Law Journal, 2002, p 1365,

[60] See M. Hildebrandt en M. Koning, Universele handhavingsjurisdictie in cyberspace?, Strafblad, 2012, pp. 195-203; Kohl, U., Jurisdiction in Cyberspace, in: Tasgourias, N and Buchnan, R. Research Handbook on International Law & Cyberspace, p 37, 38

[61] For reference: https://www.fbi.gov/news/testimony/going-dark-encryption-technology-and-the-balances-between-public-safety-and-privacy and http://europe.newsweek.com/google-microsoft-and-facebook-back-apple-encryption-battle-fbi-428014?rm=eu

[62] ibid note 41.

[63] idem

[64] Several times now we have seen suspects during interrogation express their surprise that the police were able to get to information while they took deliberate steps of choosing providers and countries with a reputation for non-cooperation.

[65] Although there are indications that there have been state attempts to do exactly that in the case of TOR. However, this method (also – see next paragraph) relies on controlling chokepoints – in this case exit-nodes. the sheer amount of infrastructure and the mesh-like global dispersion of it make it very unlikely this could succeed.

[66] For reference: The RAND Corporation, "On Distributed Communications," op cit, Vol. I, "Introduction to Distributed Communications Networks," by Paul Baran (RM-3420-PR), p. iii. Military Requirements for Packet-Switched Networks and Their Implications for Protocol Standardization, Vinton G. Cerf, Computer networks [0376-5075] Cerf, V G yr:1983 vol:7 iss:5 pg: 296

internet as a conglomerate of nation-nets that may or may not be interconnected would hamper or destroy many of the good things that the internet has brought.

With cyberspace enforcement issues on the increase it is not just countries with extremely restrictive governments that are thinking about these things. A number of Arab countries and Russia, but also countries like Brazil or Germany[67] are considering this model.

One wonders however how this method of territorialisation of cyberspace will hold up in the long run. Such territorialisation works because one can create gated choke points between one's national internet and the internet-at-large. These choke points exist because fast movement of aggregate use of cyberspace requires bandwidth currently only available through wired (fiberoptic) solutions. The increase in availability and decrease in cost for wireless techniques, like mesh networking, LiMAX, 5G, Space-X low orbit satellites and Googles internet balloons is well underway, reducing (the importance of) those chokepoints.[68] Once the ability to receive and send 'radio'waves is sufficient to maintain effective (though not necessarily fast) connections to the internet, regardless of the territorial states wishes it will be extremely hard, if not impossible, for that state to maintain its territorialisation of (their part of) cyberspace.[69]

Putative Territory; the assumption of uncertain territory

With the older principles for territorial claims largely failing to support successful claims and execution of enforcement jurisdiction in cyberspace a new contender has arrived on the field. This fairly new addition to the field of territorial jurisdictional claims is one that assumes that as long as one does not or cannot know how their 'position' in cyberspace translates to the real world and its according territorial jurisdiction, any action undertaken occurs and has effect in one's own territory. I will call this Putative[70] Territory. Putative territory as a concept suffers from a few issues which will be addressed next.

Putative territory - internal contradiction

The would-be principle of Putative territoriality suffers from an internal contradiction. However ephemeral and detached from the underlying world cyberspace may seem at times, what happens there does have an effect on the real world - sometimes a rather profound one. It is exactly such effects that are the basis of prosecution of many acts and facts that one could label as cybercrime. They are at most times also the basis for a state claiming jurisdiction under territorial principles based on the effects in it's territory of acts in cyberspace.[71]

How then would we hold to a fiction that enforcement actions in cyberspace have no likewise effects, effects which reach down from the turmoil of the all-covering blanket of cyberspace to touch the real world beneath it? Once the effects of whatever action reach the real world, they can tied to a location and with that - once more - become territorial. There is a real world exponent of the action (which is often exactly the point of enforcing), whether we can see the link between the action and it effects or not, whether it was intended or not, whether the actor was aware where the effects of his actions would materialize or not.

Putative Territoriality on the one hand has a state seeking action claiming (it's own) jurisdiction, often under the principles of constructed territoriality as basis for it's claim while the actual physical nexus is uncertain or undeterminable. At the same time, the same state denies (another state's) territoriality by ignoring the fact that while it's actions take place in cyberspace those action can, and probably will, have an effect that materialises in another states territory (since the enforcing state cannot prove presence in its own territory and technology denies easy localisation).

The result is that, at a minimum, putative territoriality as a principle is likely to create issues at the doctrinal level with one state deploying enforcement measures resulting in effects in another states legal order without the other states express consent. At the other end of the spectrum the adaptation of such a principle will lead to the negation of the very reason the principle of sovereignty is so much at the centre of the international legal order, the avoidance of (serious) conflict.[72]

---

[67] Although the primary reason given is data-protection and privacy. http://www.spiegel.de/international/germany/deutsche-telekom-pushes-all-german-internet-safe-from-spying-a-933013.html and http://uk.reuters.com/article/us-usa-spying-germany-idUKBRE99O09S20131025

[68] for reference one can take a look at Motherboard's interview with vint cerf late 2015, http://motherboard.vice.com/read/we-talked-about-refrigerators-with-vint-cerf-father-of-the-internet. A number of these techniques are or can be made point-to-point making interception are hard to neigh impossible affairs. This characteristic is bound to have the interested attention of cybercriminals.

[69] A comparison comes to mind with 'illegal' radio broadcasts by and to the resistance during WWIIWW. There was a powerful state system that aimed to prevent all outside communication, but anyone that managed to hide and keep hidden a radio could at least receive, possible send, information in and out of the controlled area.

[70] In the sense of 'assumed to exist' (even if this may not actually be true) see: http://dictionary.cambridge.org/dictionary/english/putative

[71] As we saw in the paragraph about the unexceptionalist approach any cybercriminal that keeps his wits about him creates physical and jurisdictional distance between his acts, his equipment, his proceeds and his victims.

[72] Ryngaert, C.M.J, Jurisdiction in International Law (2nded) , Oxford University Press, 2015 p 29, 32-34

Putative territory – burden of proof

If one ignores the internal contradiction Putative Territory does present a solution to the twin conundrums of whether one should ask permission and, if so, whom of. By simply claiming territoriality when not presented with a clear cut (contradicting) physical nexus there is no need to seek permission as the authority rests with oneself. However, in my opinion, Putative Territory as a concept suffers from a classical logical fallacy, the burden of proof.

Jurisdiction does not just happen or exist. A sovereign state needs to claim it. When it is not claimed, it does not exist; It is merely a latent option. As such it is a positive and conscious action by a sovereign state. The state seeking enforcement is actively looking for an effect; it is not a happenstance side-effect. The effects this state seeks through enforcement, but also the accompanying (unintended) side-effects, caused by law enforcement personnel of a state, are directly attributable to the enforcing state as effectuation of its will. The fact is that such enforcement does not operate in a vacuum and may (more likely: will) -considering the fact that locality could not be determined in the first place- have an effect on the internal legal order of another state.

As we saw in previous paragraphs international law does not outright forbid the claiming of jurisdiction with regards to prescription without a permissive principle, but State practice shows that states indeed do expect to see claims of jurisdiction backed by a applicable principle as well as a ´legitimate´ interest in asserting it.[73]

Regardless of the previous international law does clearly and unambiguously forbid enforcement[74] activity in another states territory barring a permissive rule. From the standpoint of enforcement this permission really boils down to that's states permission to do so (or in lieu of that, that state undertaking action on behalf of the state seeking enforcement).

Though old, the Lotus verdict is the defacto standard of international law with regards to (criminal) enforcement jurisdiction and to this day incontrovertibly and unambiguously forbids intervention in another states legal order through the enforcement of one's own laws.

Since it is the state seeking enforcement making a claim to jurisdiction under territory and wishing to cause an effect, it is it's burden to prove it in fact has authority, not for another party to disprove it.[75] Otherwise, if enforcement is performed unilaterally -undertaken without that state's express permission- the likely effects occurring in that other states internal legal order can hardly be interpreted as anything other than a wilful breach both of that state's sovereignty and the principle of non-intervention.

From the above the conclusion can be drawn that a burden of proof on the state seeking enforcement is most in line with doctrine, jurisprudence and state practice. The problem is, it cannot be proved, which was the trouble to begin with.

Putative territory – strategical ignorance

Finally, the concept of putative territoriality allows for much leeway in strategizing by the state seeking enforcement. Exactly how much effort would a state's law enforcement branches need to expend in trying to figure out the nearest physical nexus? Is it enough to not ignore blatant indications? Or to make a cursory check for obvious signs? Does one needs to run down WHO-IS[76] information and try and figure out the legal seat of service or provider? Is one obliged to refrain from any kind of action until territory can be determined? Is it allowed to 'hack' a server or service to find out the territorial authority to be addressed?

Different states are bound to have different opinions on the matter. They may even have different opinions at different times, depending whether they are on the giving or receiving end of such enforcement activity.[77] The state seeking enforcement can never adjust it's activities to match the territorial state, because that still needs to be determined. In short: one could never do it right, and that may be excuse enough to not even try.

The (un)tenability of Putative Territoriality

Even if we were to agree that -notwithstanding a few glaring doctrinal and factual issues- a practical solution could be found in a principle of Putative Territoriality there is little indication that states would actually accept such a solution. Anecdotal stories persist of states deliberately looking the other way when another

[73] Ryngaert, C.M.J, Jurisdiction in International Law (2nded) , Oxford University Press, 2015, p 38- 40
[74] See note 35
[75] The Lotus case, notes 26 & 33 versus the Harvard Draft Convention on Jurisdiction with Respect to Crime note 29
[76] Who-Is is a domain name lookup service, in which for any domain name on the internet registered "owner", registrar, tech and abuse contact, and other useful information; for the more technically oriented: RFC 3912, WHOIS protocol specification, https://tools.ietf.org/html/rfc3912
[77] This is not merely theoretical: Ad-hoc subgroup on Transborder Access and Jurisdiction, report: Transborder access to data and jurisdiction: Options for further actions by the T-CY, T-CY (2014)16, Council of Europe, 03-12-2014, p 13

nation breaches their sovereignty whilst enforcing their criminal law through cyberspace.[78] There are no states on record agreeing to such a practice, so far as it exists. In most such cases, at the very best, there seems to be a "on the down-low" situation, the fact of it's occurrence only known between practitioners (in different states) that have found reasons to trust each other. This is definitely not the same as an official state position sanctioning such actions and therefore we are a far cry from a newly emerging rule of (customary) international law. On the other hand, as we saw above, there is plentiful hard evidence that states are increasingly asserting full 'sovereignty in cyberspace'. This quashes any hope that for the foreseeable future of a rule of customary international law might be developing that -those factual and doctrinal issues- would allow treatment of cyberspace as a kind of 'unregulated commons'[79] that is a vessel to each state enforcement wishes.

If we rephrase the jurisdictional assertion with which we started of this paper as a question

May one assume to be operating within one´s own territory and therefore one´s own jurisdiction in cyberspace if one cannot determine the physical nexus to ones 'position' in cyberspace?

the answer to this question must be a clear "no" for the reasons described above. Absence of knowledge of territory does not equal absence of territory or the absence of intervention into another states legal order and sovereignty in case of (coercive) enforcement measures. If we do not allow claims from ordinary citizens as to a lack of knowledge regarding the law as a defence then how could we acknowledge similar claims from law-enforcement professionals? Ignorantia Terrae Non Excusat!

Conclusion

At the end of this paper a summary of findings is in order. The first is that despite an alleged lack of qualitative proof, there is a problem with enforcement in cyberspace. There are many reasons why such numbers would be underreported, while at the same time there are both quantitative and qualitative indications that a problem indeed exists, even if we can't 'prove' how big the problem exactly is.

The second is that the strength of jurisdictional claims based on territory makes it logical that states would prefer to find ways to claim their jurisdiction under that principle. Once established, the next logical step then is for states to try to cast their enforcement activity as territorial. Logical because, while it perhaps does not require a permissive rule to establish jurisdiction, international law does prohibit intervention in another states affairs. An expression of enforcement jurisdiction in another states territory would, in most cases, amount to such an intervention. This would leaving a state seeking enforcement but not wanting to break the principle of non-intervention reliant on another state's assistance. This reliance does not exist when the enforcement activity can be construed as territorial.

The third finding is that while there are powerful motives for framing cyberspace as territorial, cyberspace has been and remains inherently non-physical and technological progress causes it to become ever more tenuously connected to specific parts of its infrastructure. This poses major challenges in the translation from physical location to cyberspace location and back, challenges that reverberate in any claims of enforcement jurisdiction based of territoriality. This (increasing) unterritoriality diminishes both the potential of an Unexceptionalist approach as well as the actual territorialisation of Cyberspace. Therefore these old solution are not likely to be sufficient to solve enforcement issues in cyberspace.

The fourth conclusion is that that the new kid on block for the territoriality claims in cyberspace that I have called Putative Territoriality fares little better. There are (at least) three solid reasons that we have explored in this paper for this.

---

[78] when talking to law enforcement officials end prosecutors off the record – they are often retellings of heard stories though so actual prevalence is neigh impossible to find out. One case that has be made very public so it can safely be referenced is the so-called Operation TORpedo. For reference see: http://www.wired.com/2014/08/operation_torpedo/.
Another public example: http://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers
Another activity regularly heard about is logging into a mail server abroad with proper (i.e. the same one the suspect would use) credentials – but without the suspects permission - to get access to the content of the e-mail box. This is an activity that is heard more often – likely due it's simplicity in execution and likely lack of collateral effects

[79] See Dan Hunter, Cyberspace as Place and the Tragedy of the Digital Anticommons, 91 Cal. L. Rev. 439, 469–75 (2003), Hildebrandt, M. Extraterritorial Jurisdiction to Enforce in Cyberspace? Bodin, Schmitt, Grotius in Cyberspace, University of Toronto Law Journal, 2013 p 222-224

Firstly Putative territoriality suffers from an internal inconsistency that cannot be solved. States seeking enforcement regarding acts in or through cyberspace often rely on harmful territorial effects to claim jurisdiction *and* present a sufficient ´legitimate interest´. At the same time states relying on this principle as a basis for enforcement would have to deny the same (similar) territorial effects likely to occur in another state as a result of their enforcement efforts.

Next is the fact that a state claiming jurisdiction on the basis of Putative territoriality would wrongfully place a burden of proof on the other party. Both doctrine and state practice still unambiguously forbid the deployment of any kind of state power, let alone criminal enforcement activity, into another states sovereign sphere. Since it is the state seeking enforcement that is acting, it falls to that state to prove its action is not forbidden and thus permissible.

Finally claims based on putative territoriality go against the international legal order of sovereign states as the use of the principle (too) easily creates a method for plainly ignoring sovereignty-related issues. Should a state deploy enforcement measures without the other states express consent this raises, at minimum, issues at doctrinal level. At the other end of the spectrum adaptation of such a principle will lead to negation of the very reason as to why the principle of sovereignty is so much central to the international legal order, the avoidance of (serious) conflict. At the same time the recent trend is, as we saw, toward assertion of sovereign exclusivity in cyberspace, not away from it.

These reasons combined quash any hope for a foreseeable future in which a rule of customary international law might be developing. A rule that through this new would-be principle would -despite a few rather glaring factual and doctrinal issues - allow for treatment of cyberspace as a kind of 'unregulated commons' that would be a vessel to each state's enforcement wishes.

The result of the above is that we must come to the conclusion that while we are indeed in need of a legal construction to deal with enforcement problems on the internet, it can neither be found in the older attempts to territorialize cyberspace nor in this new attempt through a claim of uncertain territoriality that I have called Putative Territoriality.

Outro

The topic this paper was written to address the concept what I will shortly paraphrase as "putative territoriality in cyberspace". The paper only sets out what is wrong with this presumption of territoriality, not how an answer to the problem of enforcement in cyberspace may be reached. Both the length of a paper suitable for a conference as well as the fact that my Ph.D. research is not complete prevent me from attempting to do so - though I certainly have a few thoughts on the matter which I'll gladly share with you at the conference. More research is definitely needed and your presence at this conference shows an interest in tackling this problem. One suggestion I would like to make is to take a step back from many of the things we have all learned to accept as certain and unchangeable in international law and to try and stop shoehorning cyberspace into (ever more tenuous) fictions of territoriality. It will never truly fit comfortably and the attempt renders examination of other avenues of solution that much harder.

If we are to truly discuss how to create effective enforcement of laws on the internet it is, in my opinion, of eminent importance we stop playing hide and seek behind redefinitions of longstanding concepts of international law. Instead we should look for a direction forward that embraces the fact that a territorial nexus is ever less forthcoming in cyberspace, both as a 'place delit' and as the location of enforcement action. Only then we can start to discuss how we will deal with a future in which states will have to accept that, especially in cyberspace, many actions take place that affect their legal order and persons and assets within their territory, but where enforcement is beyond their territorial reach. Even though this is sometimes disputed we will also have to deal with the fact that legal assistance, while valuable and by no means obsolete, does not always provide the solutions we need, both in content but certainly not in speed.

I will certainly continue my research into the matter and I would like to take this opportunity to solicit your help with my further research. If you have experience with or have (reliably) heard things about (unilateral) cross-border enforcement activity in (cyber-)investigations please find me out and talk to me. While I have no intention of doing a quantitative study into them for the reasons detailed in the introduction, I am looking for qualitative information about occurrence and prevalence. Any information you may share with me will of course, in line with this conferences' Chatham House rules, be confidential unless otherwise agreed.