Regional Courts in Regional Organizations:

An enhanced judicial cooperation, or the failure of international law?
The counter-terrorism case-study,
amidst field particularisms and globalised cyber-attacks

SECOND PART AND CONCLUSIONS

Olesya DOVGALYUK
BSc Student in Politics and International Relations, SPAIS, FSSL, University of Bristol (UK)

Riccardo VECELLIO SEGATE
MSc Candidate in European and Global Governance, SPAIS, FSSL, University of Bristol (UK)

London
August 2017

OUTLINE CONTENTS

PART II: POSSIBLE SOLUTIONS FOR PROSECUTION & CYBERSECURITY

I think it is natural that every country has to take care of its interests, but there are some interests that are common to all countries [1]

Cyber-space is too important, both economically and culturally, to simply allow market forces to shape its development [2]

Introduction 2.0: a note of caution on the terminology and structure

In what follows we will look at different examples of judicial response to the emergent cyberthreats. However, several points should be made to set correct expectations of the forthcoming analysis and make the choice of cases and examples somewhat clearer to the reader. One is the nature of judicial bodies we scrutinise, which might – and rightfully so – strike one as a very patchy by the virtue of their mandates and powers. As commonly occurs in legal scholarship, we come across a definitional issue that ROMANO highlighted when outlining what constitutes an international judicial organ and what does not. Precisely, for him an international judicial institution has to be a permanent body issuing legally-binding decisions 'established by an international legal instrument', not an 'institutional framework and a roster of experts for ad hoc arbitration'[3], which automatically excludes all Arbitration Courts, including the Hague-based PCA, and ad-hoc tribunals, from his final list.[4] As seen from the criteria, Romano focuses on the courts with supranational jurisdiction, which means the International Criminal Court – present in one of the sections of our article – because of its complementary jurisdiction[5] is also excluded. In this article, however, we alternately discuss *both* national and international judicial institutions; and, in the light of the ill-developed legislation around cyberspace, it is not our goal to adopt strict criteria to decide which bodies fall under the latter category.

What we aim to do is to look at recent responses to cyberoffences and threats from judicial and quasi-judicial institutions around the world, compare different legal philosophical perspectives on this ambiguous category of crime, and try to "predict" the next steps to tackle

---

[1] George Soros, interviewed by Davis Smiley, available online at: http://www.pbs.org/wnet/tavissmiley/interviews/philanthropist-george-soros/

[2] KAMAL, Ahmad (2005) *The Law of cyberspace: an invitation to the table of negotiations*, Geneva: United Nations Institute of Training and Research, available online at: https://www.un.int/kamal/sites/www.un.int/files/The%20Ambassador%27s%20Club%20at%20the%20United%20Nations/the_law_of_cyber-space.pdf [p. 158]

[3] ROMANO, Cesare P. R. (1999) 'The proliferation of international judicial bodies: the pieces of the puzzle', *New York University Journal of International Law and Politics,* 31: 709-751, available online at: http://www.pict-pcti.org/publications/PICT_articles/JILP/Romano.pdf [pp. 713-714]

[4] ROMANO's final list of judicial institutions included: International Court of Justice (ICJ); International Tribunal for the Law of the Sea (ITLOS); European Court of Human Rights (ECtHR); Inter-American Court of Human Rights (IACtHR); Court of Justice of the European Communities (ECJ) together with its Court of First Instance (CFI), now Court of Justice of the European Union (CJEU); Central American Court of Justice (CACJ); Court of Justice of the Andean Community (TJAC); Court of Justice of the European Free Trade Association (EFTA CJ); Court of Justice of the Benelux Economic Union (Benelux CJ); Court of Justice of the Common Market for Eastern and Southern Africa (COMESA CJ); Common Court of Justice and Arbitration of the Organization for the Harmonization of Corporate Law in Africa (OHCLA CJ); Court of Justice of the Arab Maghreb Union (AMU CJ); Judicial Board of the Organization of Arab Petroleum Exporting Countries (OAPEC JB) – see ibid. [pp. 715-717]

[5] see: https://www.icrc.org/eng/assets/files/other/145-172-solera.pdf

it. As there already exist comparative studies of regional cybercrime legislation[6], some geographical regions are not covered here since this paper's objectives were to look at the most interesting state practices, to draw on certain regional differences and, more broadly, to sketch the relation between the global and regional judiciary in the field of cybersecurity. Secondly, throughout this analysis we mention several law enforcement measures as examples of international cooperation; this should not appear as a deviation from the analytical chain, since preventive policies and legal frameworks will serve as grounds for future practice of prosecution, now scarce on examples. Lastly, due to this scarcity of examples, we will try to fill in the gaps by drawing parallels with the existent areas of threat in IL: for instance, 'international law on, and the international legal controversies related to, counter-terrorism [can be applicable] in various ways to potential acts of cyber terrorism [with] [c]ertain malicious cyber activities by terrorists [potentially falling] within the scope of existing anti-terrorism treaties'.[7]

1. Bilateral and multivalent arrangements

Although traditional bilateral agreements come in the form of Mutual Legal Assistance (MLA) and extradition agreements as some of the most widely-practiced forms of interstate cooperation, the latter range more widely, including information-sharing practices, continuous dialogues and meetings, statements and Memoranda of Understanding (MOUs), as well as creation of norms and ethical standards (see fig. 1 in the Appendix).[8] For instance, in the field of introducing e-commerce coordination, ICT section focuses on 'exploring synergies between the "Digital India" initiative and the EU's "Digital Single Market"'.[9] New Delhi's bilateral relations with ASEAN and the ASEAN Regional Forum (ARF) are also 'particularly valuable

---

[6] see e.g. http://www.ryerson.ca/tedrogersschool/privacy/documents/Ryerson_International_Comparison_ofCyber_Crime_-March2013.pdf and, from a more historical perspective: http://cybercrimelaw.net/documents/cybercrime_history.pdf

[7] FIDLER, David P. (2016) *Overview of International Legal Issues and Cyber Terrorism*, Study Group on Cybersecurity, Terrorism, and International Law, International Law Association, available online at: https://www.scribd.com/document/273605594/Study-Group-Overview [pp. 3-4]. In the US, for instance, in addition to the already-developed penal law on computer-related crimes, foreign cyberattackers could be prosecuted under the *Military Commission Act* (2009) if they 'have engaged in hostilities against the United States or its coalition partners' and based on the grounds that 'Manual for Military Commissions (MMC) regards terrorism as a war crime' (LEBOWITZ: http://illinoisjltp.com/journal/wp-content/uploads/2013/05/Lebowitz.pdf, pp. 102-103). As such, a cyberattacker could be prosecuted for war crimes if the elements of the crime of terrorism are present, thanks to the general wording of the Act, subject to interpretation on what exactly constitutes a hostile act against the US. Additionally, terrorist attacks (geopolitical risks) have been identified as the closest to cyberattacks, a threat from the different category of global risks (technological risks), by the World Economic Forum – see: http://reports.weforum.org/global-risks-2017/global-risks-landscape-2017/; at the moment, however, there is 'no universal instrument against terrorism [that would] impose an obligation on States to enact legislation specifically targeting the use of the Internet by terrorists' (https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, p. 31), although many encourage such actions (see e.g. *Report of the UN Secretary-General S/2015/366*, Art. 79).

[8] for a comprehensive overview of the main international cybersecurity modes of cooperation, see: RADUNOVIĆ, Vladimir, and the DiploFoundation team (2017) *Towards a secure cyberspace via regional co-operation: overview of the main diplomatic instruments*, available online at: https://www.diplomacy.edu/sites/default/files/Diplo%20-%20Towards%20a%20secure%20cyberspace%20-%20GGE.pdf

[9] PAWLAK, Patryk (2016) *EU-India Cooperation on Cyber Issues: Towards Pragmatic Idealism?*, Istituto Affari Internazionali, available online at: http://www.iai.it/sites/default/files/iaiwp1636.pdf [p. 5]

for the EU as it aims to promote more actively the development of CBMs [Confidence-Building Measures] in the region'.[10]

Most of the joint operations and MLA-enabled extradition of cybercriminals appearing on the publicly available media, and thus available as examples for this paper, usually involve the US (likely due to its being the most targeted country by cybercriminals, as well as a broader reach of Western media across the world, which – often disproportionately – gives it an advantage in agenda-setting): for instance, in cases *US v Nikita Vladimirovich Kuzmin*, *US v Deniss Calovskis,* and *US v Mihai Ionut Paunescu* where three individuals collectively created a virus, a fake bank website and a "'bulletproof host", two were extradited to the United States from Latvia and Romania, while the third one was arrested in the US.[11] Some of the successful intelligence exchange practices for cybercrime prosecution purposes have been seen between the US and the UK. In addition to the elaborate defense and prevention mechanisms put in force in the Obama-Cameron agreement framework, such as US-CERT and CERT-UK coordination, we can see initial steps towards judicial cooperation in the related crimes as part of the Mutual Legal Assistance between the two countries. One of them is the recent operation *R v Ackroyd and Others* (of the "LulzSec" group), where FBI cooperated with their UK counterparts in identifying and bringing to justice members of the criminal group committing offences 'relating to DDoS attacks against various targets including the CIA (USA), the UK Serious Organised Crime Agency (SOCA) and News International; and unauthorised access and modification to websites including sites belonging to Sony, Twentieth Century Fox and the NHS'.[12] There were, however, a number of controversial cases, such as a still-disputed and appealed request for the extradition of Lauri Love[13], a Finnish-British citizen diagnosed with Asparagus who repeatedly hacked US governmental websites, and a similar previous case of Gary McKinnon, who was not extradited on human rights grounds.[14]

An interesting dynamic in the approach to collective cybersecurity can be observed between the US, China and Russia. Cooperation between the "strategic competitors"[15] US and China has seen many ups and downs, subject to the levels of confidence in each other's true intentions[16] and alignment of the positions. On the one hand, Beijing (taking existing

---

[10] ibid. [p. 6]

[11] see: https://www.unodc.org/cld/case-law-doc/cybercrimecrimetype/usa/2013/us_v_nikita_vladimirovich_kuzmin_us_v_deniss_calovskis_and_us_v_mihai_ionut_paunescu_.html and https://www.youtube.com/watch?v=yk32_8UFL8w ; in case of the (allegedly) Latvian national Deniss Calovskis, the defendant also appealed to the ECtHR, which subsequently found the extradition compatible with the European Convention on Human Rights.

[12] see The Crown Prosecution Service on *Computer Misuse Act* (1990): http://www.cps.gov.uk/legal/a_to_c/computer_misuse_act_1990/

[13] LUSHER, Adam (2016) 'Lauri Love verdict: British hacker who breached US defence systems to be extradited despite Asperger's', *The Independent*, September 16, available online at: http://www.independent.co.uk/news/uk/home-news/lauri-love-extradition-verdict-hacker-loses-case-us-aspergers-latest-news-a7311351.html

[14] ROZENBERG, Joshua Rufus (2012) 'Gary McKinnon: Theresa May had no choice but to use human rights grounds'*, The Guardian*, October 16, available online at: https://www.theguardian.com/law/2012/oct/16/gary-mckinnon-theresa-may-human-rights

[15] POLLPETER, Kevin (2004) *U.S.-China Security Management: Assessing the Military-to-Military Relationship*, Santa Monica (California): RAND Corporation [p. 41]

[16] for instance, to counterbalance US alliances in East Asia which PRC sees as a foothold for containment of China's power, the latter has engaged with two other core regional players, Japan and South Korea, in a Trilateral Cyber Policy Consultation, where representatives have 'confirmed that the three countries continue to exchange in the area of cyber affairs on the diplomatic channel' to increase mutual assistance in 'regional and international fora' (http://www.mofa.go.jp/press/release/press4e_001474.html)

counterterrorism strategies as an example) has been a timely and active contributor to the "Global War on Terror", for instance by signing a bilateral declaration of principles 'allow[ing] the US Customs agents to inspect containers' in Shanghai and Shenzhen ports.[17] Additionally, it acted as a regional mediator to ease tensions between India and Pakistan, ensuring that 'the conflict in Kashmir does not disrupt operations in Afghanistan'[18], a move the US have recognised as supportive of and complementary to the American strategy. Simultaneously, however, opposition to any interventionist interference in Iraq, Iran and North Korea has shown China's persistent perception of the Washington's covert aim as that of promoting a preferred global order and preventing a potential Chinese regional dominance. This explains why, despite the two countries have signed an agreement on cybersecurity in 2015, committing to

> 'provide timely responses to requests for information and assistance concerning malicious cyber activities[;] refrain from conducting or knowingly supporting cyber-enabled *theft of intellectual property*[;] pursue efforts to further identify and promote appropriate norms of state behavior in cyberspace within the international community[;] and establish a high-level joint dialogue mechanism on fighting cybercrime and related issues'[19],

tensions remain, and cyberoffences (like the operation "Aurora" by China against the thirty-four US companies[20]) are carried out on a regular basis, even though it is difficult to always clearly discern any government's hand behind them. A pronounced case of Su Bin (2014), decided by the US District Court of the Central District of California, which included conspiracy to get 'unauthorized access to protected computer networks in the United States, including computers belonging to the Boeing Company in Orange County, California, to obtain sensitive military information [primarily about the F-35, C-17 and F-22 military jets – added by us] and to export that information illegally from the United States to China'[21] ran relatively smoothly, with a successful extradition of the criminal from Canada to the US and the admittance of the conspiracy by Mr Bin. However, no mention was made of the People's Liberation Army ("PLA"), China's armed forces, despite the information revealed upon the release of the Vancouver court's "books of record" that the USDOJ accused China-based co-conspirators for being affiliated with the military.[22]

Tracing the record of China's cyber espionage this way allows to shed light on the fact that '[t]he Chinese landscape, frequently characterised as monolithic and rigidly state-directed,

---

[17] *supra,* note 15 [p. 31]

[18] *supra,* note 15 [p. 31]

[19] ROLLINS, John W. (2015) *U.S.-China cyber agreement*, CRS Insights: IN10376, Washington, DC: Congressional Research Service – the Library of Congress, available online at: https://fas.org/sgp/crs/row/IN10376.pdf [emphasis added]

[20] BROWN, Gary, and YUNG, Christopher D. (2017) 'Evaluating the US-China Cybersecurity Agreement, Part 2: China's Take on Cyberspace and Cybersecurity', *The Diplomat*, January 19, available online at: http://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-2-chinas-take-on-cyberspace-and-cybersecurity/

[21] The US Department of Justice (2016) *Chinese National Pleads Guilty to Conspiring to Hack into U.S. Defense Contractors' Systems to Steal Sensitive Military Information*, Press Release, March 23, available online at: https://www.justice.gov/opa/pr/chinese-national-pleads-guilty-conspiring-hack-us-defense-contractors-systems-steal-sensitive

[22] FREEZE, Colin (2016) 'China denies role in cyberhack that stole U.S. military aircraft secrets', *The Globe and Mail*, January 22, available online at: https://www.theglobeandmail.com/news/national/china-denies-role-in-cyberespionage-campaign-that-stole-us-military-aircraft-secrets/article28354342/

is composed of a wide range of groups'[23]: on the one hand there are traditional 'squads of PLA soldiers whose full-time jobs are to hack away at the West's secrets'; on the other – 'unaffiliated, arms-length hackers who sell their wares to Chinese firms'[24]; when the two, however, are the same professionals acting in line with the strategic interests of the PRC government, their extradition or domestic prosecution under China's criminal law becomes difficult to imagine (unless under exceptional circumstances significantly threatening China's reputation). The same is observable in the Russian-Chinese dynamic, where Russian defense, nuclear, and aviation industries are being targeted by Chinese hackers despite the accords concluded by both sides.[25] However, one noteworthy aspect of the Russia-China's agreement on cybersecurity comes from its norm-building nature (discussed further in this article).

Altogether, it can be seen through this selection of examples that states have been diplomatically active in the face of accelerating levels of threat springing from the misuse of IT and computer networks. It is important to note though that such mutual assistance will often vary on a case-by-case basis, and is not as much a binding agreement as a gesture of good relationship and strategic alignment between the two or more states in a certain aspect of national/international security. Thus, as seen from the recent investigation by the UK intelligence into the terrorist attack in Manchester, the leakage of the perpetrator's identity in the main US media[26] can make the UK government think twice before sharing sensitive data with their foreign partners, which can potentially damage an operation and subsequently put citizens' lives in danger. Bilateral agreements commonly represent symbolic diplomatic steps of temporary appeasement or bettering of interstate relations; in the case of cybersecurity, unless some process of attribution is legitimised and grounds for further retribution are created, agreements will leave the governments free to violate their overly-general commitments. Despite all this, as we will see further, bilateral arrangements in some contexts – if not in most – will still play a major role for the judicial cooperation in the framework of the binding multilateral agreements.

2. Global supranational judiciary

To understand the inadequacies of the attempts to arrange 'the maintenance of international public order' one, as JENKS states, only had to look at the *Annual Digest of Public International Law Cases* to be 'impressed by the number of unsettled points in even those parts of international law which have [previously] suffered [the] least'.[27] More than six decades later,

---

[23] FireEye (2016) *Red Line Drawn: China recalculates its use of cyberspace espionage*, Special Report, available online at: https://www.fireeye.com/content/dam/fireeye-www/current-threats/pdfs/rpt-china-espionage.pdf [p. 15]

[24] FREEZE, Colin (2016) 'Chinese soldiers implicated in U.S. military hacking case', *The Globe and Mail*, January 18, available online at: https://www.theglobeandmail.com/news/national/chinese-entrepreneur-living-in-canada-implicated-in-us-military-hacking-case/article28253148/

[25] KRAVCHENKO, Stepan (2016) 'Russia More Prey Than Predator to Cyber Firm Wary of China', *Bloomberg*, August 25, available online at: https://www.bloomberg.com/news/articles/2016-08-25/russia-more-prey-than-predator-to-cyber-firm-wary-of-china

[26] see: https://www.theguardian.com/uk-news/2017/may/23/trump-administration-manchester-bomber-name-leak

[27] JENKS, Clarence Wilfred (1943) 'Regionalism in International Judicial Organization', *The American Journal of International Law*, 37(2): 314-320 [p. 316]

too little has changed. 'Supranational dispute settlement […] starts from the notion that international law binds nonstate actors as well as their governments' with 'jurisdiction [which] is parceled out to coequal institutions, with no higher appellate authority to resolve jurisdictional conflicts'[28]: in other words, to count as such, supranational institutions are supposed to show practice of permanent and binding judgements (reflecting ROMANO's criteria above) and preliminary rulings, nonstate access, and direct effect with no opt-out option for the prospective perpetrators.[29] It is important to clarify what is meant by the practice of binding judgements, as it could imply both governments' compliance with the Court's rulings, and effectiveness of the latter; at the same time, distinction between the two is a crucial one. In particular, high levels of compliance do not necessarily signify that the international rules guiding physical and juridical persons' behaviour are fair and effective[30]; contrastingly, rulings with low compliance 'might be quite effective if they engender some modification of state [and individual] behaviour'.[31]

Few existent courts, however, can be described as having a supranational authority. ECtHR and CJEU (operating regionally) are recognised closest to the ideal model (which is, however, due in large to many conditional factors, such as relative EU normative and juridical homogeneity – called "European legal space"[32] – and high standards of the rule of law). CJEU is often considered a role model for other regional courts due to its significant supranational powers enforced through the mechanisms of strong political representation (which outbalance weak political delegation). In addition, it is often referred to as convincing supportive argument in defence of the second-generation trade-related tribunals and arbitration bodies (discussed in section 3) as it has also had, as a part of the joint European project, the liberal market-shaping element aimed at 'freeing […] individuals from collectively imposed obligations'[33]. Yet, we need to remember that it is 'not easily transferable nor necessarily appropriate for other regions'[34]: effectiveness of the EU judicial system has been largely due to the already-developed network of independent national and EU courts, 'an expert, active legal profession [,] the proper implementation and enforcement of CJEU rulings before national courts by their *agreement* or *acquiescence'* (emphases added by us) in the absence of a compelling Union power to enforce CJEU rulings.[35] The question of choosing between a strong executive and (soft trust-building) legislative power will thus be answered differently as we switch from one region to another and face different political and judicial systems as well as the dissimilar cultures historically underpinning

---

[28] BEZUIJEN, Jeanine, COMAN, Emanuel, DERDERYAN, Svet, and HOOGHE, Liesbet (2014) 'Designing Third Party Dispute Settlement for International Organizations', San Francisco (California): ISA Annual Convention, available online at: http://wp.peio.me/wp-content/uploads/2014/04/Conf7_Hooghe-Bezuijen-Derderyan-Coman-30.08.2013.pdf [pp. 2 & 12]

[29] ibid. [pp. 11-12]

[30] an example of this is the relationship between the Russian Constitutional Court and the ECtHR – see, e.g.: http://www.cisarbitration.com/2017/01/25/russian-constitutional-court-denies-enforcement-of-echr-decision-on-yukos/

[31] HELFER, Laurence R. (2014) 'The Effectiveness of International Adjudicators', in ROMANO, Cesare, ALTER, Karen J., and SHANY, Yuval (eds) *The Oxford Handbook of International Adjudication*, Oxford: Oxford University Press [p. 465]

[32] see: http://www.ejls.eu/12/146UK.htm

[33] HÖPNER, Martin, and SCHÄFER, Armin (2012) 'Embeddedness and Regional Integration: Waiting for Polanyi in a Hayekian Setting', *International Organization*, 66(3): 429-455 [pp. 432; 434-435]

[34] European Commission (1995) 'II. European community support to integration efforts throughout the developing world' in *European Community support for regional economic integration efforts among developing countries: Communication from the Commission,* available online at: http://ec.europa.eu/development/body/legislation/recueil/en/en13/en131_2.htm

[35] TATHAM, Allan Francis (2010) 'Exporting the EU Model: A Judicial Dimension for EU International Relations?', *LXIII Studia Diplomatica,* available online at: http://www.ies.be/files/Tatham-B5.pdf [p. 2]

present institutions. Given this, some reasonably doubt feasibility of adjusting CJEU model to external contexts since 'it is a regional European exception'[36] with constituent states 'belong[ing] to the same legal family [where] the communication between highest courts forms part of a formal or informal network'[37] (this will be even more so after "Brexit"), which could have limited applicability in other (more heterogenous, for example) regional settings. Of relevant global courts neither ICJ nor ICC can overshadow that of national jurisdiction, the former predominantly issuing non-binding advisory rulings for the cases referred by international organizations or other international tribunals or states[38], and the latter being complementary to domestic legislations, despite the Prosecutor having more judicially-active mandate to open investigations into the actions of or against its member-states' nationals. The scholarly popular idea of empowering ICJ as a universal judicial body takes its roots in the Court's universal clientele, provided through the mechanism of automatic accession by the UN members, which at first appears a huge *ex ante* benefit, as many specialised judicial organisations already consist of (almost exclusively, if not considering states with limited recognition, such as Palestine) UN state-parties. An additional reason is its role as an adjudicator in highly-contentious cases, e.g. Yugoslavia's application against NATO, the river boundary between Botswana and Namibia, and the questions of Nuclear Proliferation. However, as the Court operates in a 'highly sensitive and politically charged' environment, its rulings are often too general to have a precedent impact.[39] A more feasible role for the Court would be to 'promot[e] a greater degree of reflexivity in the part of specialised judicial tribunals […] and emphasise[ ] the importance of relations of mutual scrutiny' between the latter.[40] Yet, if – as opposed to having a more coercive power – the ICJ will preserve its mainly advisory function, the likelihood of other judiciary institutions (either regional or more local) requesting for external mediation by the UN Court is questionable, while adjudicating legal inconsistencies – with regards to our article's focus, for example, sprung from different interpretations of the terms "terrorism" and "cyberterrorism" – in case of imposing a legal obligation without the consent of at least one party has a danger of violating the Vienna Convention on the law of treaties.[41]

Interpretation in the light of lacking universal definition will be a crucial practice, as the inefficacy of the multidimensional fragmentation of International Law along the issue-area (human rights, trade, maritime, environment), geopolitical/cultural (European, Chinese, Socialist, Shariah), and private-public lines is perceived to be a direct consequence of an absent general global legislative body to negotiate the conflict of laws.[42] This is the case for

---

[36] BORN, Gary B. (2012) 'A New Generation of International Adjudication', *Duke Law Journal*, 61(4): 775-879 [p. 869]

[37] GELTER, Martin, and SIEMS, Mathias (2015) 'Networks, Dialogue or One-Way Traffic? An Empirical Analysis of Cross-Citations Between Ten of Europe's Highest Courts', in ANDENAS, Mads, and FAIRGRIEVE, Duncan (eds) *Courts and Comparative Law,* Oxford: Oxford University Press, pp. 200-212

[38] see: http://www.ejil.org/pdfs/9/3/662.pdf

[39] LANG, Andrew (2013) 'The role of the International Court of Justice in a context of fragmentation', *International & Comparative Law Quarterly*, 62(4): 777-812 [p. 804]

[40] ibid.

[41] *Vienna Convention on the law of treaties*, May 23, 1969 (registered *ex officio* on January 27, 1980), United Nations Treaty Series, available online at: https://treaties.un.org/doc/Publication/UNTS/Volume%201155/volume-1155-I-18232-English.pdf

[42] UNGA (2006) 'Fragmentation of International Law: difficulties arising from the diversification and expansion of International Law' – *Report of the Study Group of the International Law Commission* (finalised by KOSKENNIEMI, Martti), available online at: http://legal.un.org/ilc/documentation/english/a_cn4_l682.pdf [pp. 8-10]

cyberterrorism as well: prominent advocates, such as Stein Schjølberg[43], stress the need for the hierarchisation of the judiciary institutions under an overarching coordinator as the only effective measure to address unacceptable juridicial relativism and ensure effective prosecution for violating immunity of critical data systems and public infrastructure and threatening citizens' safety. The first embodiment of such a coordinator is the projected International Criminal Tribunal for Cyberspace.

2.1 International Criminal Tribunal for Cyberspace

Defining cyberspace as 'the fifth common space, after land, sea, air and outer space'[44], Schjølberg stresses the necessity of creating an International Criminal Tribunal for Cyberspace with jurisdiction over the violations of the "international cybercrime legislation", executed with the purpose of:

> destroying, damaging or rendering unusable critical communication and information infrastructures, causing substantial and comprehensive damage to or interference with national security, civil defense, public administration and services, public health and safety, or banking and financial services.[45]

Some questions, however, remain unanswered: would this Tribunal, following the draft Statute guidelines which were carefully designed to avoid the flaws found in other treaties (Rome Statute in particular), have primacy over domestic courts (Article 9)[46] or, in case prospective members do not agree to recognise such a mandate, it will have a positive complementary nature? If the latter is the case, then it will face even more complex issues than the ICC: the geopolitical boundaries of the cyberspace are at best extremely uncertain, at worst inexistent. As a result, outlining guidelines for the Prosecutor to draw a distinction between the offences under the national jurisdictions (those "not-to-be-interfered-with") and those posing threat to the international community could prove extremely challenging, despite the proposed independence of his or her office 'not only [from] the Security Council, but also [from] any state or any international organisation or other organs of the Tribunal'.[47] Supposing, however, the Tribunal is given its principal universal juridical authority: will its judgements in the face of numerous nuances of overly-complex legislative overlaps (not lastly because of the mentioned geographical uncertainties which hinder identification of laws to adopt in the juridical process) allow for judicial interpretation, similar to the practice of Islamic qiyās in deductively interpreting hadiths with reference to Quran[48] or, say, the Common Law tradition prone to judicial activism in analysing precedents and referring to customs?

---

[43] Judge Stein SCHJØLBERG. a retired Norwegian lawyer, is one of the founders of the harmonization of national criminal law on computer crime. Over his career he has been dealing with cybercrime issues either analytically or practically, as a member of the International Think Tank on Global Court Technology, the Chairman of the global High-Level Experts Group (HLEG) on cybersecurity, and an extraordinary Court of Appeal Judge in Norway (among many other positions).

[44] SCHJØLBERG, Stein (2012) 'Recommendations for potential new global legal mechanisms against global cyberattacks and other global cybercrimes' – *A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group*, available online at: http://www.cybercrimelaw.net/documents/ICTC.pdf [p. 3]

[45] ibid. [p. 9]

[46] ibid.

[47] *supra,* note 44 [p. 20]

[48] GLENN, Patrick H. (2012) 'An Islamic Legal Tradition: the law of a later revelation', in *Legal Traditions of the World: Sustainable Diversity in Law* (5th edition), Oxford: Oxford University Press [pp. 185-186]

Another problem is, of course, the one already facing almost all international institutions entrusted with the supposedly-universal mandate: it is the absence of an effective enforcement mechanism to foster rulings in case of non-compliance. Sanctions and collective "condemnation" by the member-states towards the guilty party (we are talking about state actors now), can prove effective, but in case the guilty party is a powerful state, which can survive such a "blockade" (say, the US or, despite the obvious damage to its economy, Russia), it can have reverse effects and only foster further aggression. Thus upholding of the Law has to go hand-in-hand with an integrated yet mutually-unbiased and independent relationship between the judicial and enforcement elements, which further implies relation of the Tribunal with the UN Security Council, akin to the ICC-UNSC model. Additionally, the quandary of the necessary share of intelligence, caused by the *a priori* sensitive nature of the crucial for national security data, will expectedly be a significant obstacle on the way to cooperation at all levels. This has been especially true in transatlantic relations following Snowden's revelations, which have proven that '[i]n the digital era, states can be allies in the fight against cybercrime but competitors in the area of national cybersecurity' and that '[t]his potential conflict of interest or paradox – both between as well as within states – introduces many challenges in addition to the inherent complexity introduced through cyberinsecurity'.[49]

2.2 Expanding the ICC mandate

An extremely complex, but also intellectually engaging is the potential relation between the cybercrimes and the territorial jurisdiction of the International Criminal Court. As discussed above, the concept of state borders with regards to cyberattacks is blurred; it was long debated whether the prosecution of such crimes should be based on the location of original attackers, technologies/computing machines used[50] and their direct targets, or also include the victims of spillover consequences thereof. Put differently, 'the critical question is whether the Court may use constructions of qualified territoriality, in the absence of explicit legislation, to address the cyber commission of core crimes'[51], or it will stick to the conventional *lex loci delicti commissi*.

Although crimes committed through the Internet are not mentioned in the Rome Statute, Article 21(1b) allows for the reference to the customary International Law for further interpretation of crimes. The most fundamental question here is to determine whether the cybercrime in question can be interpreted in such a way as to fall under either of the crime categories under the Court's mandate. This is tricky: debates about whether, for example, cyberterrorism can in and of itself be linked to crimes against humanity or crimes of aggression (both during and not as part of the war conduct) have been ongoing. For instance,

---

[49] European Parliament (2015) *Cybersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses*, a study by Directorate General for Internal Policies, Policy Department C: Citizens' rights and constitutional affairs, available online at: http://www.europarl.europa.eu/RegData/etudes/STUD/2015/536470/IPOL_STU(2015)536470_EN.pdf [p. 18]

[50] In this regard hackers' and cybercriminals' use of botnets is a growing concern for the identification of the source of the crime and identity of the criminal; additional issue poses the question of whether the territorial jurisdiction can be asserted by 'localising the cyber-commission of a core crime in whole or in part within the territory of States Parties' – VAGIAS, Michail (2016) 'The Territorial Jurisdiction of the ICC for Core Crimes Committed Through the Internet', *Journal of Conflict & Security Law,* available online at: https://academic.oup.com/jcsl/article-lookup/doi/10.1093/jcsl/krw021 [p. 523]; for more general discussions from the same Author, see https://openaccess.leidenuniv.nl/bitstream/handle/1887/17669/Kopie%20van%2015976970002-bw.pdf?sequence=3.

[51] ibid. [p. 526]; for more on the concept of the qualified territoriality see GILBERT, Geoff (2006) *Responding to International Crime,* Leiden: Martinus Nijhoff Publishers [chapter 3]

in 1954 International Law Commission *Draft Code of Offences against the Peace and Security of Mankind*, 'never formally adopted by the General Assembly or in treaty form, […] [t]errorism was explicitly linked to the concept of aggression'.[52] The type of aggression referred to, however, is that exercised by states only, thereby leaving individual acts of "private terrorism" out of the Code's scope.

Despite this ambiguity, the matter jurisdiction of the ICC[53], as well as of any other judicial institution and International Law itself is flexible, as seen from the recent policy papers expressing the initiative to add 'acts of environmental destruction, illegal exploitation of natural resources and land-grabbing, [and] human rights abuses to the crimes'[54] under the ICC mandate, not to mention the destruction of cultural heritage.[55] Thus, if initiated and supported by the Prosecutor, crime of terrorism (whether conventional or perpetrated via cyberspace and computer machines) could also be incorporated into the list of crimes – under, for instance, the broad category of crimes against humanity. Consequently and building upon this, prosecution based on national belonging of the 'e-perpetrators' to the Member State of the Rome Statute or the location of the victim/target of the attacker could be used as grounds for invoking an investigation. There are, however, rightful doubts about the willingness of the Member-States (especially after the "secession" of Russia and some African states in 2015-2016), already cautious of the Prosecutor's judicial activism, to be bound by such a mandate.[56] Amending jurisdiction to add the crime of cyberterrorism thus has to be approached carefully, not to trigger another wave of withdrawals and an institutional crisis.

Global-level solutions do not end with just ICTC and ICC[57]: however, despite the elaborateness and certain soundness, they are often controversial when it comes to politicised matters. It also has to be said that arguments based on the idea of 'cyberspace as a "global

---

[52] SAUL, Ben (2005) 'Attempts to define "Terrorism" in International Law', *The Netherlands International Law Review*, available online at: http://www.cicte.oas.org/olat/documents/Defining%20TERRORISM%20in%20International%20Law.pdf [p. 66]

[53] see: https://civilprocedure.uslegal.com/jurisdiction

[54] DOVGALYUK, Olesya, and VECELLIO SEGATE, Riccardo (2017) *From Russia and beyond: the ICC global standing, while countries' resignation is getting serious*, Bologna: FiloDiritto, available online at: https://www.filodiritto.com/documenti/2017/articolo-russia-riccardo-vecellio-segate-filodiritto-2017.pdf [p. 18]

[55] http://www.ohchr.org/Documents/Issues/CulturalRights/DestructionHeritage/NGOS/A.P.Vrdoljak_text1.pdf [p. 11 ff.]; http://heritage.sense-agency.com/assets/Uploads/sg-7-05-gerstenblith-destruction.pdf [p. 386 ff.]; https://harvardlawreview.org/wp-content/uploads/2017/05/1978-1985_Online.pdf ; and GREEN MARTÍNEZ, Sebastián Axel (2015) 'Destruction of Cultural Heritage in Northern Mali: A Crime Against Humanity?', *Journal of International Criminal Justice*, 13(5): 1073-1097

[56] To date,Turkey has been advocating for terrorism to be included in the list of crimes under the ICC jurisdiction – see Statement by the Head of the Turkish Delegation, Mr İsmail Aramaz, at the Kampala ICC Review Conference (2010): https://asp.icc-cpi.int/iccdocs/asp_docs/RC2010/Statements/ICC-RC-gendeba-Turkey-ENG.pdf; it is unclear, however, how Turkey would react to adding the "cyber"-dimension to the criminalisation of terrorism in the Court.

[57] CREEKMAN, for instance, suggested a multilateral extradition agreement – which, despite all the unlikelihood to be adopted as a solution, remains in theory a valid option. See: CREEKMAN, Daniel M. (2002) 'A Helpless America? An Examination of the Legal Options Available to the United States in Response to Varying Types of Cyber-Attacks from China', *American University International Law Journal*, available online at: http://digitalcommons.wcl.american.edu/cgi/viewcontent.cgi?article=1223&context=auilr. Another suggestion for enabling prosecution of foreign perpetrators under domestic jurisdiction is 'adding extraterritorial application to current domestic criminal laws bearing on cyberattack' – see: STOCKTON, Paul N., and GOLABEK-GOLDMAN, Michele (2014) 'Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat', *Stanford Law & Policy Review*, 25(2): 211-268 [p. 211]

common" seem to have somewhat failed to gather universal consent to date'[58] due to several reasons. First, despite the abstract ubiquity of cyberspace, there definitely exists 'a real-world technical infrastructure on which [it] is based, which is owned by governments[,] corporations' and individuals, and which gives states grounds to invoke principles of sovereignty and national jurisdiction; second, this infrastructure in many cases remains private property, which would have to be nationalised[59] – an idea barely acceptable in the context of 'liberalised and competitive ICT markets'[60] of today – for the truly single global regime to be created.[61] The existent discussion of global jurisdiction 'comes partly as a response to those who believe that legal harmonisation is, or would be, impracticalities aside, the Holy Grail to many online regulatory problems. It is not', and for good reasons: the diversity of regulations and sensitivity of the problem area make many envision for the Criminal Tribunal for Cyberspace the same destiny as for the ICC.[62]

3. Complex multilateral cooperation: intra- and inter-regional networks

If, alternatively, fragmentation is indeed beneficial as more accurately representing pluralistic international legal order and creating opportunities for a dialogue among the actors pursuing different political interests, the next question arises: how would judicial authority be "parcelled-out" without the *opinio juris* expressed by all the actors engaged first? Taking as an example the field of International Criminal Law, we can claim that it 'is mostly an exercise in altruism' for the stable and well-off democracies, while the developing countries, perceived by the former as 'consumers of international criminal justice' and suspicious of any intrusion into their sovereign affairs[63], have shown – in best-case scenarios – reluctant commitment to binding universal treaties, cautious enough to make appropriate reservations as acts of self-defence. South African Development Community Court project, "victimised" by the governments of its own member-states, whose commitment to national land interests and principles of elites' mutual (often racially-underpinned) support prevailed over the protection of their subjects' rights, clearly shows the imbalance between the developed South Africa

---

[58] ZIOLKOWSKI, Katharina (ed.) (2013) 'Peacetime regime for state activities in cyberspace: International Law, International Relations and Diplomacy', *NATO CCD COE Publication*, available online at: https://cryptome.org/2014/01/nato-peacetime-cyberspace.pdf [pp. 194-195]

[59] Following the WannaCry ransomware that, among other damages, hit hard the UK's healthcare service NHS, there have been discussions of granting the government significant regulatory powers over the Internet. This follows an introduction of the the new *Investigatory Powers Act,* which allows the government to obtain vast amount of communications data. See: http://www.independent.co.uk/life-style/gadgets-and-tech/news/theresa-may-internet-conservatives-government-a7744176.html?amp; for the text of the Act: http://www.legislation.gov.uk/ukpga/2016/25/ (especially section 61).

[60] *SADC ICT Consumer Rights and Protection Regulatory Guidelines,* adopted by SADC Ministers responsible for ICT, in Luanda (Angola): 2010, available online at: http://bit.ly/2rtRH5g [p. 5]

[61] ibid.

[62] KOHL, Uta (2014) 'Barbarians in Our Midst: "Cultural Diversity" on the Transnational Internet', *European Journal of Law and Technology*, available online at: http://ejlt.org/article/view/304/426

[63] ANDERSON, Kenneth (2009) 'The Rise of International Criminal Law: Intended and Unintended Consequences', *The European Journal of International Law*, 20(2): 331-358, available online at: https://academic.oup.com/ejil/article/20/2/331/500849/The-Rise-of-International-Criminal-Law-Intended [p. 333]

(widely perceived as one of the most democratic regimes on the continent[64]) and other Community members, which exaggerates the asymmetry in cost-benefit distribution.[65] Similarly, the failure of regional integration (mostly trade and economy-oriented, but in judicial matters as well) within the Commonwealth of Independent States has been 'due to objective reasons, in particular the fact that Russia's political, economic, population and territorial potential greatly exceeded those of the other member states' in addition to individual members' dissimilarity in foreign policies, which made the relations in Eurasian Economic Community (EurAsEC), the Collective Security Treaty Organisation (CSTO) and the Common Economic Space (CES) superficial.[66]

Exacerbating the situation is the fact that national security interests and uneven development are not the only factors distancing regions from each other. Divergent legal traditions bring an element of a cultural schism, which is often more difficult to bridge than conflicting national interests: while the latter can be approached through the accommodation of the core requirements in a somewhat balanced manner, the former raises the issue of legitimacy more than that of legality, shaking the very grounds of judicial morality. Attempts to find a compromise in the field of law has resulted in the theoretical acceptance of universalisation and tolerance as two alternative – yet mutually incompatible, as many dichotomous concepts in Western legal philosophy – approaches to address divisions.[67] Both solutions have their flaws: universal approach, grounded in the possibility of 'accommodation with other complex traditions'[68], raises questions in the light of internal ambiguity within the legal traditions themselves, which has led to the conflict and fragmentation within the latter and subsequently 'create[d] doubts about external expansion'.[69] Tolerance, on the other hand, appears a passive tactic of 'allowing diversity to sustain itself, at its might'.[70]

While we consider pro-active multivalent thinking as necessary in resolving essentially normative conflicts, if it turns out to be a "mission-impossible", alternative incentives for regional cooperation might come into play. A recurring dynamic can be observed, which shows us that in certain types of organizations rulings tend to have a more binding nature, thereby ensuring a greater effectiveness and stability. These are:

1) **numerically smaller organisations** or organisations with **geographically-proximate**[71] members (e.g. Benelux, EFTA). Regional courts, associated with these institutions or operating within and across the scope of their membership 'would presumably have a greater concentration of prosecutors, staff, and judges from the local community, thereby

---

[64] HULSE, Merran (2012) 'Silencing a Supranational Court: The Rise and Fall of the SADC Tribunal', *E-International Relations*, October 25, available online at: http://www.e-ir.info/2012/10/25/silencing-a-supranational-court-the-rise-and-fall-of-the-sadc-tribunal/

[65] JACKSON, Paul (2012) 'Regional Security in Sub-Saharan Africa', in BRESLIN, Shaun, and CROFT, Stuart (eds) *Comparative Regional Security Governance*, Abingdon-on-Thames: Routledge

[66] KONOŃCZUK, Wojciech (2007) 'The failure of integration. The CIS and other international organisations in the post-Soviet area, 1991-2006', *OSW Studies*, available online at: https://www.osw.waw.pl/sites/default/files/prace_26_1.pdf

[67] GLENN, H. Patrick (2014) 'Reconciling legal traditions', in *Legal Traditions of the World: Sustainable Diversity Law* (5th edition), Oxford: Oxford University Press

[68] ibid. [p. 375]

[69] ibid. [pp. 376-378]

[70] ibid.

[71] *supra,* note 31

augmenting the perceived domestic legitimacy of the tribunal'.[72] Along with the legitimacy benefit come significantly reduced costs, ensuring greater independence of regional arbitration in contrast to global multilateral institutions dependent on member-states' financial support, which can be used for political purposes. Finally, the very logic behind such a middle-scope authority, local enough to have a power grip yet allowing for multi-actor participation, resonates with what was designed by BUZAN and WÆVER as Regional Security Complex Theory, which states that, against the broader "Clash-of-Civilizations" background, countries form security subsystems by allying with other regional actors in a way that the level of their mutual connectedness cannot be analysed without one another.[73]

2) **trade-related institutions based on regional economic integration agreements (REIAs)**, especially between the economically-interdependent countries, whose emergence also implied punitive mechanisms coined by BORN as the "second-generation tribunals", success whereof 'directly contradicts central claims by skeptics of the efficacy and value of international adjudication and, more broadly, international law'.[74] This category encompasses the Appellate Body of the WTO, NAFTA Tribunal and the like, which reflect the Global Political Economy approach in seeing the simultaneity and mutual reinforcement of regional and global integration. However, this mutuality as well cannot be taken for granted: other scholars suggest that 'the multilateral venue of legal rulemaking is seriously undermined and forum shopping is triggered – bilaterally, regionally or through new plurilateral initiatives within clubs of countries, unattached to any international organization'.[75] This suggests that "regionalisation" and "supranationalisation" of cross-national laws can also be understood as antithetical more than supporting.

(Relative) independence of these international commercial and investment arbitrations 'brought along […] to settle disputes between members arising out of the implementation of the agreements'[76] in the aftermath of the decline of the Marxist ideas and '[t]he triumph of the market-economy paradigm and free-trade doctrines'[77], arguably has a critical impact on the scope and boldness of their actions, which have proven broadly successful thanks to the 'procedural and factfinding regimes[,] designed to satisfy users' expectations – including those of state parties – and, at the same time, to provide mechanisms for addressing dissatisfaction'.[78] These mechanisms, however, arguably require some contextual framework to operate, such as high levels of states' democraticness and comparatively symmetric (i.e. non-dominated in a hegemonic manner) share of power among the members[79], due to the need 'to determine the relative weight of independence and interdependence [between the tribunals and

---

[72] BURKE-WHITE, William W. (2003) 'Regionalization of International Criminal Law Enforcement: a Preliminary Exploration', *(Paper 959)* Faculty Scholarship, *Texas International Law Journal* [p. 737]

[73] BUZAN, Barry Gordon, and WÆVER, Ole (2003) *Regions and Powers: The Structure of International Security*, Cambridge: Cambridge University Press [pp. 41; 44]

[74] *supra,* note 36 [p. 867]

[75] BURRI, Mira, and COTTIER, Thomas (2012) (eds) *Trade Governance in the Digital Age: World Trade Forum*, New York City: Cambridge University Press [p. 6]

[76] *supra,* note 3 [p. 735]

[77] ibid.

[78] *supra,* note 36 [p. 874]

[79] *supra,* note 31

the members as well as among the latter – added by us] in order to delineate the explanatory power of diffusion effects'.[80] They also require specific legislation; progress in this field is already noticeable, if we look at the UNCTAD map of 'e-commerce legislation in the field of e-transactions, consumer protection, data protection/privacy and cybercrime' adopted throughout the world (see fig. 4 in the Appendix, as well as, for instance, World Bank reports). Nevertheless, since 'globalization — of economics or crime — calls for regional solutions to common problems', blank spaces such as some African states, where little binding legislation has been adopted in this field, leave loopholes for the terrorists to freely engage in illegal activities (facilitation of illegal financial flows etc.). To tackle this issue, regional trade institutions could provide more comprehensive solutions to regional law enforcement.[81]

Further cooperation will also depend on the legal tradition underpinning state's judicial system: for instance, there might be some difference in engagement of the Prosecutors in Civil Law and Common Law traditions, the former being generally prone to have a more active role in early investigative initiatives, and the former relying more on the police for evidence.[82] This is, of course, a generalisation, which would be unfair to adopt as a lens in predicting judicial behaviour across the world. Nevertheless, some cases prove that contradictions between supranational and domestic legislation do prevent states from participating in international efforts: an example of this is the US's not being 'a party to an additional Protocol on Cyber Crime adopted by the Budapest Convention in 2006, which criminalized online dissemination [of] xenophobic or racist material, due to concerns of conflict with the First Amendment to the US Constitution'.[83] The observation should still be kept in mind also for the cases involving two states with different legal systems (including Religious Law, such as Sharia, Jewish Halakha, Modern Hindu Law and so forth), which are poorly or not at all integrated in the harmonised regional international legal framework.

Taking all this into account, the article will proceed by briefly looking at the features of regional judiciaries and recent cybersecurity developments in several regions. It is important to remember, however, that success of regional integrations is only partial. As potential scope of cyberterrorism and other cyber- and computer-facilitated offences encompasses truly vast territories and travels miles within seconds, cooperation between the national and regional judiciaries to 'facilitate the judicial aspect of extradition requests'[84] and ensure effective prosecution is needed, because 'a single court that challenges an executive will fail, whereas when multiple courts coordinate their responses, there is more likelihood of executive deference to courts in general'.[85] Examples of such cooperation are currently limited in number, compared to the *threat-prevention* mechanisms (predominantly under executive

---

[80] RISSE, Thomas (2015) 'The Diffusion of Regionalism, Regional Institutions, Regional Governance', *Paper presented at the EUSA 2015 Conference*, Boston, March 5-7, available online at: https://eustudies.org/conference/papers/download/32

[81] *supra*, note 72 [p. 745]

[82] GRABOSKY, Peter Nils (2007) 'Requirements of prosecution services to deal with cyber crime', *Crime, Law and Social Change*, 47 [p. 206]

[83] DE MELLO BARRETO, João Paulo (2015) 'Comments Off on Global Cyber Crime: Catching Overseas Hackers', *Columbia Undergraduate Law Review*, available online at: http://blogs.cuit.columbia.edu/culr/2015/04/28/global-cyber-crime-catching-overseas-hackers/

[84] UNSC (2016) 'In Fight against Terrorism, Security Council Adopts Resolution 2322 (2016), Aiming to Strengthen International Judicial Cooperation', *Meetings Coverage and Press Releases*, December 12, available online at: https://www.un.org/press/en/2016/sc12620.doc.htm

[85] GINSBURG, Tom (2009) 'National Courts, Domestic Democracy, and the Evolution of International Law: A Reply to Eyal Benvenisti and George Downs', *The European Journal of International Law*, 20(4): 1021-1026 [p. 1022]

authorities) such as networks of Computer Emergency Response Teams. Yet this is precisely the reason why this grey area, important for the future development of Public International Law in general, will be shed light upon further below.

3.1. Sub-Saharan Africa: East, and down the South

Legal history of sub-Saharan Africa has, as that of many post-colonial spaces, been subject to drastic changes over relatively short periods of time, often not allowing legal traditions to evolve at a natural pace, as was – and still is – the case for the diverse customary law seen then by the Europeans as hindering national unity, lacking juridical character and slowing modernisation processes.[86] Roots of the consequent lack of regional cohesion lie in the combination of several factors. The first one is poor harmonisation of laws, even within smaller (sub-)Regional Economic Communities, with neighbouring states often having different legal systems.[87] Numerous – and by the virtue of their number, confusing – not-binding documents, designed as models for the binding law, are aimed to resolve the issue of regional legal integration and judicial cooperation; yet, the only binding legislation in the field of cybersecurity – the AU Convention on Cybersecurity and Personal Data Protection (2014)[88] – has inherent flaws in it. Its primary inefficiency is not the fact that at the moment it only enjoys eight signatories and no ratifications, which makes the prospects of Convention getting in power (which requires 28 ratifications) look a distant-future phenomenon; the main problem of the Convention is its unfitness for the levels of legal advancement in Africa, met by its comparable sister – Budapest Convention in Europe.[89] Despite that the latter was numerously considered as 'offer[ing] a good base on which to frame laws that deal with the challenges posed by cybercrime'[90], there are several issues to be taken into account if modelling the AU guidelines on the CoE (Council of Europe) Convention. Specifically, as opposed to providing a platform for the cases when two states do not have a mutual legal agreement on extradition, the AU document encourages[91] states to develop national legislative mechanisms – absent in many African states (see fig. 2 & 3 in the Appendix) – and subsequently *individually* establish bi- and multilateral agreements with other states.[92] This might mean that, unless such legislation alongside with the MLA and extradition agreements is implemented, states with no legislation criminalising cyberoffences can serve as safe havens for foreign perpetrators, if we are to

---

[86] BENNETT, T. W. (2006) 'Comparative Law and African Customary Law', in REIMANN, Mathias W., and ZIMMERMANN, Reinhard (eds) *Oxford Handbook of Comparative Law,* Oxford: Oxford University Press, pp. 641-673 [p. 662]

[87] e.g. mixed Belgian Civil and English Common Law in Rwanda and Burundi, and Statutory and Common Law, mixed with elements of tribal and Islamic law in Kenya (in the East Africa/African Great Lakes region)

[88] *AU Convention on Cybersecurity and Personal Information,* adopted by the XXIII ordinary session of the Assembly in Malabo (Equatorial Guinea), 2014, available online at: https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

[89] ORJI, Uchenna Jerome (2014) 'Multilateral Legal Responses to Cybersecurity in Africa: Any Hope for International Cooperation?', *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, available online at: http://bit.ly/2sazNkM

[90] MWAITA, Patrick, and OWOR, Maureen (2013) *Workshop Report on Effective Cybercrime Legislation in Eastern Africa,* Dar es Salam (Tanzania), 22-24 August, available online at: https://rm.coe.int/16802f2349 [p. 2]

[91] *supra,* note 88 [Artt. 24-27]

[92] *supra*, note 89 [p. 111]

follow the principle of dual criminality, mentioned in the Convention.[93] However, here comes the tricky part: Budapest Convention clearly states that, in case two states have no agreement on extradition or one of the states has not criminalised a specific cybercrime in question, the Convention itself could serve as a legal basis for extradition claims; no such mechanism is developed in the AU Convention.[94] As a regional-level binding legislation it failed to provide truly regional-level solutions, remaining a broad guide for cooperative actions among individual states yet not providing a ground for this cooperation in case relevant legislation is absent in a specific state, or if members involved do not have harmonised laws or assistance agreements on the matter.

Combined with the poor "cyber hygiene" (many governments reportedly use unsophisticated and hackable templates for their online platforms[95]), this will not prevent or slow down the already-pessimistic dynamic of an estimated $2b of losses in 2016 and generally growing cybercrime levels[96], with the continent scoring highest in detected exploits, malware and botnets per organization (see fig. 5 in the Appendix). While transborder cybercrime court cases are still very limited in general, in sub-Saharan Africa, according to the ITU comparative analysis of the African regional organizations, 'no case related to telecommunication was brought to any of [the African] courts'[97], including courts in Eastern, Western, Northern and Southern Africa, despite the obvious presence of cases to choose from.[98] And the problem does not (only) lie in the lack of judicial cooperation (despite recently positive dynamics in the Human Rights cases[99]); the reality is more prosaic: as many countries' reports state, some cyberoffences are not criminalised in their national legislation, a priori leaving prosecution with their hands tied (or, at least, more tied than preferred, since some cybercrimes can be interpreted with provisions for other criminal acts). A case worth mentioning with regards to the "transnational" nature of crime is the arrest and prospective trial of a Ugandan, Ronnie Nsale, and another Kenyan by the Kenyan police on the suspicion of 'hacking into databases

---

[93] these fears were mirrored in relation to other crimes committed in the Great Lakes Region such as terrorism, as well as gravest crimes under International Law by the International Centre for Transitional Justice (ICTJ):

> Despite the expression of these political commitments, the investigation and prosecution of national and international crimes continue to face numerous challenges, including the lack of appropriate judicial cooperation between the States of the region. Obstacles to judicial cooperation continue to fuel the impunity of military leaders and other superiors who are accused of international crimes as they benefit from protection in their own State or in neighboring States.

(for the full text of ICTJ Report on the high-level conference on the regional judicial cooperation in the Great Lakes Region in Kinshasa see: https://ungreatlakes.unmissions.org/sites/default/files/judicialcooperation_greatlakes_confreport_eng_ictj.pdf, p. 3)

[94] The only AU legislation which serves as the legal basis for extradition if the two states have no MLAs or specific extradition agreements, is the *Convention on Preventing and Combating Corruption* – see: *African Union Convention on Preventing and Combating Corruption,* adopted on 1st July 2003, entered into force on 5th August 2006, available online at: http://www.eods.eu/library/AU_Convention%20on%20Combating%20Corruption_2003_EN.pdf, Art. 15(3)

[95] *Nigeria Cyber Security Report 2016*, compiled by Serianu Cyber Threat Intelligence Team in partnership with Demadiur Systems Limited and the USIU's Centre for Informatics Research and Innovation (CIRI), at the School of Science and Technology, available online at: http://www.serianu.com/downloads/NigeriaCyberSecurityReport2016.pdf [p. 9]

[96] IT News Africa (2017) 'Growth in West African Cybercrime', March 10, available online at: http://www.itnewsafrica.com/2017/03/growth-in-west-african-cybercrime

[97] ITU (2009) *ICT Regulatory Harmonization: A Comparative Study of Regional Initiatives. Harmonization of ICT Policies In Sub-Sahara Africa,* Activity G-1 of HIPSSA Project, available online at: https://www.itu.int/ITU-D/projects/ITU_EC_ACP/hipssa/docs/D_REG_HIPSSA_2010_PDF_E.pdf [p. 35]

[98] see, for instance: http://www.bbc.co.uk/news/world-africa-39351172; http://www.bbc.co.uk/news/world-africa-34830724

[99] REVENTLOW, Nani Jansen (2016) 'Press Freedom and Africa's Regional Courts: A Positive Model for Transparency and Accountability', *Just Security*, December 22, available online at: https://www.justsecurity.org/35773/press-freedom-africas-regional-courts-positive-model-transparency-accountability/

of banks, mobile phone companies [notably, Safaricom, with unspecified[100] financial losses as a result] and money transfer service providers'[101], as well as hacking into the into the Independent Electoral and Boundaries Commission (IEBC), a key electoral institution in Kenya, allegedly linked to a larger international ISIS-affiliated terrorist grouping. As the case is relatively recent, and reasonably few details have been released, there is no information about the mutual legal assistance (or mutual recognition) of the Ugandan authorities or Ugandan judiciary in data-gathering efforts (which would be of understandable interest for this article), but it is certainly only one of the forthcoming many. Though both Kenya and Uganda have a comparatively developed cybercrime legislation in the region[102], combined with the fact that this case did not require extradition and will most certainly not see the controversy in applying the objective territoriality principle – since the crime in question was aimed at and affected critical infrastructure in Kenya –, there will most certainly be less-clearcut situations (e.g. in Burundi and Tanzania which are 'at early stages in the development of legislation'[103]), which would require up-to-date and harmonised laws. One of the most prominent impediments which points at the need to amend legislation is, for instance, evidence-related controversy, which would deem procedural laws inapplicable to considerable 'electronic or other intangible evidence of cybercrime',[104] as well as the following controversy of 'unilateral cross-border searches in cyberspace', which can be potentially considered violation of sovereignty.[105]

Model Law on Computer Crime and Cybercrime (2012)[106] of the South African Development Community (SADC), on the contrary, contains regulations on electronic evidence, which makes it one of the few such legislations present worldwide covering both criminalisation and investigation of computer- and cybercrimes. However, the scope of its applicability is limited not only by the ineffective in addressing internet crimes (although visibly strengthened over the last years) national legal codes[107]; within SADC previous legislation, there are worrying contradictory provisions, such as the ones between the Protocol on Mutual Legal Assistance and the Protocol on Extradition: while the former states that mutual legal assistance in criminal matters 'shall be provided without regard to whether the conduct which is subject of investigation, prosecution, or proceedings in the Requesting State would constitute an offence under the laws of the Requested State'[108], the latter clearly adopts a principle of dual criminality, which requires the act under prosecution to be criminalised in

---

[100] ToPo News (2017) *Court orders detention of ISIS-linked terror suspects*, April 7, available online at: http://tupo.co.ke/court-orders-detention-isis-linked-terror-suspects/

[101] MUKINDA, Fred, and KAKAH, Maureen (2017) 'Detectives link Ugandan Ronnie Nsale to IEBC hacking', *Daily Nation*, April 7, available online at: http://mobile.nation.co.ke/news/-Ronnie-Nsale-to-Safaricom-and-iebc-hacking/1950946-3880474-10cb0nwz/index.html

[102] *supra,* note 90

[103] ibid. [p. 3]

[104] ibid.; an interesting *R. v. Whiteley (Nicholas)* case from the UK (1991) could serve as a precedent in the Common Law system, which saw the judges ruling out that the amendment of the files on the disk constituted damage to the hardware, as the combination of the original electronic particles of the disk was changed in the process.

[105] GHOSH, Sumit, and TURRINI, Elliot (eds) (2010) *Cybercrimes: A Multidisciplinary Analysis,* Berlin: Springer [p. 324]

[106] ITU (2013) *Computer Crime and Cybercrime: Southern African Development Community (SADC) Model Law,* available online at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/SADC%20Model%20Law%20Cybercrime.pdf

[107] The Southern Times (2015) *SADC states argued to harmonise cybersecurity laws*, May 26, available online at: https://southernafrican.news/2015/05/26/sadc-states-argued-to-harmonise-cybersecurity-laws/

[108] SADC *Protocol on Mutual Legal Assistance in Criminal Matters*, 2002, available online at: http://www.sadc.int/files/8413/5292/8366/Protocol_on_Mutual_Legal_Assistance_in_Criminal_Matters_2002.pdf [Art. 2(4)]

both the requesting and the requested state.[109] And while MLA by no means equates to extradition of criminals, being often limited to the intelligence share, it gives states space to deny even that for political reasons. Which is why, despite the overall recognised progressive approach to the cybersecurity, SADC regulatory mechanisms and guidelines are not legally-binding, which brings us back to the point one: the basis for future collaboration is created, but the substance is still absent. Additional factor of the de facto suspension (in 2010) of the previously-mentioned SADC Court also provides little space for the judicial discretion in transnational cybercrime and computer crime instances.

To sum up, while we are definitely seeing national attempts to produce comprehensive anti-cybercrime legislation[110], most of it concerns the economic side of it, protecting – or striving to protect – e-transactions and online banking among others; the reality so far confirms our previous suggestion that it is economics that will drive regional communities' legislative and judicial advancements. Subregional and regional response mechanisms, such as CERTs[111], are still heavily underdeveloped, which has to be addressed in addition to amending accordingly the AU Convention, an instrument potentially serving as one of the legislations for reference in prosecution of cybercrimes in the continental African Court of Justice and Human Rights – 'the first court of its kind in the world at the regional level with the objective of addressing both human rights and ICL'.[112] At the moment 'the establishment of [harmonised] east African e-government and e-commerce programmes [which] are expected to cover data security, network security, cyber-crime, information systems and electronic transactions'[113] and judicial cooperation in the spirit of Article 126 of the East African Community Treaty[114] is still – as stated by the representatives of the Community itself – a "work in progress".[115] Once amended to address legal issues in the region, the African Union will have to simultaneously take an additional practical step and establish an official regional-continental CERT[116] to manage public and private sector cybersecurity coordination, as well as queries from individuals, facilitate experience and knowledge exchange, and help to establish new national centres which Africa is currently lacking.

---

[109] SADC *Protocol on Extradition*, Luanda, signed 2002, entry into force 2006, available online at: http://www.sadc.int/files/3513/5292/8371/Protocol_on_Extradiction.pdf [Art. 3]

[110] for instance, recent approval of a new *Computer and Cybercrime Law*, which criminalises 'cyber offences such as computer fraud, cyber-stalking, child pornography and unauthorized access to computerised systems', by the Kenyan Cabinet, to be passed as a Law – see: http://www.techweez.com/2017/04/07/computer-cybercrimes-bill-2017-kenya-approved/ ; for the text of the Bill: http://www.mygov.go.ke/wp-content/uploads/2016/07/MOICT-PUBLICATION-READY-COMPUTER-AND-CYBERCRIMES-BILL-2016-1-1-1.pdf

[111] present only in 12 countries in sub-SaharanAfrica: Burkina Faso; Cameroon; Cote-d'Ivoire; Ghana; Kenya; Mauritius; Nigeria; Rwanda; South Africa; Uganda; United Republic of Tanzania; and Zimbabwe – see: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/CIRT_Status.pdf

[112] ADDIS, Tefera Degu (2015) 'Some reflections on the current Africa's project on the establishment of African Court of Justice and Human Right (ACJHR)', available online at: https://africlaw.com/2015/06/29/some-reflections-on-the-current-africas-project-on-the-establishment-of-african-court-of-justice-and-human-right-acjhr/#more-957

[113] Mr Tumwebaze, Ugandan minister of the ITC, quoted in https://www.scmagazineuk.com/kenya-set-to-pass-cyber-crime-bill-as-east-africa-seeks-legal-harmony/article/652047/

[114] *The Treaty for the Establishment of the East African Community*, signed on November 30, 1999, entered into force on July 7, 2000, available online at: http://www.eac.int/sites/default/files/docs/treaty_eac_amended-2006_1999.pdf [Art.126]

[115] ACHIENG, Robert (2015) *Regional Case Study: Cyberlaw Reform in the EAC*, Expert Meeting on Cyberlaws and regulations for enhancing e-commerce: including case studies and lessons learned, March 25-27, available online at: http://unctad.org/meetings/en/Presentation/CII_EM5_P_RAchieng_en.pdf [p. 11]

[116] The already-existent AfricaCERT has been established by a group of private actors, see: http://wacren.net/en/content/africa-training-initiative-and-africacert-sign-strategic-agreement

3.2 MENA region: private sector initiatives in Qatar and UAE

Cybercrime is an alarming threat for the Middle East: second most reported economic crime in the region, it is especially present in the member-states to the Cooperation Council for the Arab States of the Gulf (GCC), whose prosperous oil-fuelled economies become attractive targets for cyberattacks. Most notorious instances so far include Flame virus attacks across the region; hacking of Aramco through Shamoon virus for cyber espionage purposes, which – the company being state-owned – some consider an attack against Saudi Arabia itself[117]; and Iran's nuclear facilities being hit by Stuxnet worm, the American-Israeli cyber-weapon[118] released together with the implementation of dramatic Mossad incursions against Tehran's nuclear program, which continued the assassination of world-leading scientists (already known to be a core asset of Tel Aviv's secret services over the previous decades).

To both maintain favourable environment for investment and increase cyber-resilience among these constant turbulences, a notable private-sector-led approach of free economic zones has been taken across the GCC states, most widely in UAE and Qatar.[119] Dubai Healthcare City and Dubai International Financial Centre (DIFC), and Qatar Financial Centre (QFC) among other GCC free zones have enacted data protection laws, modelled on the EU Data Protection Directive, that regulate 'the processing, storage and transfer of personal data'[120] by organizations operating within their specific jurisdiction. They also allow for the data transmission only if the jurisdiction within which the recipient operates provides adequate data protection – in the case of DIFC (whose laws are modelled on the UK Common Law), curiously, UAE legislation is not considered "adequate"[121] – or to respond to law enforcement or state requests, protect legitimate interests of Data Controller and in other circumstances outlined in Article 12 of the DIFC Data Protection Law.[122] Contrary to popular belief, businesses in free zones are still obliged to comply with the UAE Federal law, such as Federal Publications and Publishing Law (1980)[123], e-Commerce Law and Cybercrime Law (2006). But since no harmonised intra-GCC law governing data protection has been designed as of today, and many Arab countries lack legislation protecting data processing (except for Tunisia and

---

[117] KSHETRI, Nir (2016) 'Cybersecurity strategies of Gulf Cooperation Council Economies', *Georgetown Journal of International Affairs*, available online at: http://journal.georgetown.edu/cybersecurity-strategies-of-gulf-cooperation-council-economies/#_ftnref2

[118] see further: BALZACQ, Thierry, and CAVELTY, Myriam Dunn (2016) 'A theory of actor-network for cyber-security', *European Journal of International Security*, 1(2): 176-198 [pp. 191 ff.]

[119] the already-existent Arab Investment Agreement and the established Arab Investment Court, while progressive steps, only protected Arab citizens owning Arab capital and investing it in the territory of any State Party but the one (s)he is a national of; free zones, on the contrary, allow for equal protection to foreign investors.

[120] *supra,* note 117

[121] for the list of legislations considered adequate by DIFC see: https://www.difc.ae/files/7914/5449/6593/Data_Protection_Regulations.pd [p. 19]. UAE legislation on cybercrime, interestingly, is considered the most advanced in the region. The latest *Federal Decree-Law No. 5* of 2012 was comprehensively designed to fight IT crimes and criminalise 'transmitting, publishing or promotion of pornographic material, gambling activities and indecent acts'. It was later amended to also 'ensure alignment between the UAE legislation and relevant international treaties, such as the Budapest Convention on Cybercrime' (http://www.executive-magazine.com/cybersecurity/cyberthreats-in-the-gcc-and-middle-east)

[122] *Data Protection Law DIFC Law No. 1 of 2007 (Amended by Data Protection Law Amendment Law DIFC Law No. 5 of 2012)*, available online at: https://www.difc.ae/files/5814/5448/9177/Data_Protection_Law_DIFC_Law_No._1_of_2007.pdf [Artt. 11-13]

[123] consensually interpreted as applicable to publication in all formats, printed and digital.

Morocco), Free Zones jurisdictions should be viewed as additional layers of protection against data misuse.[124]

A distinct category of cyber-criminals – not only in the Middle East, but worldwide generally – are terrorist organizations. As opposed to cyber-pirates, who prevalently use their hacking skills for economic purposes, for the former stakes are often of political nature. And even though both are not (yet?) capable of effecting destructive cyber- terror attacks against critical infrastructure, ISIL's "virtual planners" have been successful in *computer-facilitated* terrorism in the form of networking and "crowdsourcing" for potential affiliates to secure their foothold abroad.[125] As aggressive interpretations of Islam play one of the most important roles in the recruitment and radicalisation processes, Arab states' most "burning" bucket-list point is, on the one hand, to develop a counter-narrative as an ideological component of the battle, and ensure timely regional and global responses. Regionally, the Arab Convention on Combating Information Technology Offences by the League of Arab States (2010) can be considered a benchmark piece of legislation, binding member-states to criminalise any illicit use of computer networks and ICT and to 'increas[e] the punishment for traditional crimes when they are committed by means of information technology'[126], further specifying that its jurisdiction covers crimes: committed in several states; planned in the state other than the state of perpetration; involving criminal groups exercising activities in more than one state; or, cybercrimes having severe consequences in more than one state. Coupled with the advanced provisions on judicial cooperation in the Arab Guiding Law on International Cooperation in Criminal Matters, it could provide a solid basis for further judicial cooperation between the Member-States, and potentially serve as a model for other states following Islamic legal tradition, both in itself and through the body of prospective jurisprudence. There is no denying, however, that the Arab region presently displays a weakly-developed interstate judicial apparatus to enact such legislation on a supranational level: the original LAS project of an Arab Court of Justice that would facilitate harmonised revision of Shari'a principles in Islamic Law through *ijtihad* (legal reasoning) and develop a comprehensive body of Islamic International Principles[127] has gone silent at the end of the last century, while the currently-envisioned Arab Court of Human Rights is being criticised for many flaws, absence of individual access chief among them.[128] This is also emphasised by the fact that, contrary to the other "major" monotheistic religions, Islam does is not presided over by a central normative authority able to smooth the sectarian divisions and understandings of Islam itself.[129] Institution- and norm-

---

[124] For more on the free zones, GCC laws on cybersecurity and comparisons with Western legislation, see KSHETRI, Nir (2016) *The Quest to Cyber Superiority: Cybersecurity Regulations, Frameworks, and Strategies of Major Economies,* Cham: Springer International (especially chapter 11).

[125] VIDINO, Lorenzo, MARONE, Francesco, and ENTENMANN, Eva (2017) *Fear Thy Neighbour: radicalisation and jihadist attacks in the West*, ISPI of Milan: Ledizioni LediPublishing, available online at: https://extremism.gwu.edu/sites/extremism.gwu.edu/files/FearThyNeighbor%20RadicalizationandJihadistAttacksintheWest.pdf [pp. 73-76]

[126] League of Arab States (2010) *Arab Convention on Combating Information Technology Offences* [Art. 21]

[127] FODA, Ezzeldin (1957) *The Projected Arab Court of Justice: A Study in Regional Jurisdiction with Specific Reference to the Muslim Law of Nations,* Dordrecht: Springer

[128] For the criticisms of the Arab Court of Human Rights Statute see *The Tunis Declaration on the Arab Court of Human Rights*: http://icj.wpengine.netdna-cdn.com/wp-content/uploads/2015/05/MENA-Arab-Court-Tunis-Declaration-Advocacy-2015-ENG.pdf.

[129] For an updated discussion on Islam and International Law, see MAYER, Ann Elizabeth (2013) *Islam and Human Rights: Tradition and Politics* (5th edition), Boulder (Colorado): WestView Press. Indeed, this book is still a valid source, although being extremely polemical and disregarding primary references which are (self-evidently) written in Arabic.

building – which a judicial reform akin to the above essentially is – is a lengthy process indeed, which often takes generations to entrench and normalise novel practices into societies; yet the speed of technological development and growing rates of digital literacy make natural pace a luxury in the case discussed.

On the subject of global cooperation, a degree of mutual assistance in law enforcement is observable in the region, and the level of recently-enacted legislation as well as technological innovation for emergency-response operations is in general high enough to allow for intelligence-sharing and coordination (and, theoretically, even extradition on the basis of dual criminality). As an example, the first joint cyber investigation between the US FBI and Attorney, and Egyptian counterparts – the so-called operation "Phish Phry"[130] – proved a successful cooperative effort, resulting in the arrest of a criminal ring operating in both countries. Cultural-political divide with the West, however, still presents obstacles to smooth and timely coordination of actions. Accelerated levels of threat have pushed some states in the MENA region to tighten their social media policies and grant their already highly-interventionist[131] governments greater oversight powers, simultaneously cutting space for public debate, one of the crucial platforms for the counter-narratives and accommodation of the excluded and particularly vulnerable categories of the population.[132] Going back to the "Phish Phry", while the intelligence-sharing part of the operation can be praised, the judicial-cooperation aspect remains either absent or covert: whereas sentencing the US criminals, chief among them Kenneth Joseph Lucas, Nichole Michelle Merzi, and Jonathan Preston Clark (who managed the network of set-up fraudulent accounts)[133], was shed light upon disproportionately little, nothing was announced concerning the fate of those arrested in Egypt.[134] Resultant apprehension between the parties and alienation from the wider global society has as one of its effects the fact that, for now, none of the Arab Middle Eastern states has tried to actively shape global norms and decision-making procedures on the Internet (Israel, not an Arab state but still a Middle-Eastern actor, is an exception as it

---

[130] MCGLASSON, Linda (2009) '"Phish Fry" Nets 100 Fraudsters: Biggest Cyber Crime Investigation in U.S. History', *BankInfoSecurity*, available online at: http://www.bankinfosecurity.com/phish-fry-nets-100-fraudsters-a-1846

[131] as one example, while European states and institutions stand by the view that Internet Service Providers (ISPs) should not be held accountable for the online content, in the Middle East responsibility for the oversight of the published information can lie within the providers, which motivates (or directly obliges) the latter to regulate the content available online. Lately, however, even in Europe the dynamic has been changing – see, for example: http://blogs.lse.ac.uk/mediapolicyproject/2016/10/20/liability-and-responsibility-new-challenges-for-internet-intermediaries/

[132] Al Arabiya (2014) *Saudi Arabia amending laws to monitor social media*, June 2, available online at: http://english.alarabiya.net/en/media/digital/2014/06/02/Saudi-Arabia-amending-laws-to-monitor-social-media.html; FRANDA also mentions, with regards to Saudi Arabia, false rumours in late 1990s of the planned white-listing policies of prohibiting all websites until proven non-offensive. The policy never came into being, with only blacklisting of certain "inappropriate" websites by the government, but it shows the perception of the extent to which Internet is not free in the KSA – see: FRANDA, Marcus F. (2002) *Launching into Cyberspace: Internet Development and Politics in Five World Regions*, London: Lynne Rienner Publishers [p. 68]; for the updated analysis of the restrictions on the Internet freedom see Freedom House country report: https://freedomhouse.org/report/freedom-net/2016/saudi-arabia

[133] official charges included wire and bank fraud; computer fraud; and money laundering conspiracy among others – for the full text of the indictment see: https://www.wired.com/images_blogs/threatlevel/2009/10/indictment_operation-phish-phry1.pdf

[134] HALEY, Kevin P. (2011) *Operation Phish Phry - Revisited*, Symantec Official Blog, July 22, available online at: https://www.symantec.com/connect/blogs/operation-phish-phry-revisited

has been more compliant with the international standards in order to pioneer in high-tech development[135]). Their voice and experience will nonetheless have to be heard, sooner or later.

3.3 South-East Asia

According to PICT (Project on International Courts and Tribunals), regional courts and tribunals (excluding ad-hoc/hybrid bodies) are currently present in Europe, Americas and Sub-Saharan Africa; indeed, Asia – just as the previously-analysed Middle East and North Africa – appears to be in the embryonic stage of developing its regional judicial apparatus. The dynamic is not surprising as Asian 'is less adversarial and litigious than Western legal culture'[136], which is also reflected in limited power in the intergovernmental organizations, the most bright example whereof is ASEAN: and as the most frontline example of Asian cooperation platforms, ASEAN is thus worth examining on the subject of cybersecurity and cybercrime response policies first, before coming back to the question of judiciary.

Far from being a 'terrain for a democratic peace'[137] like the European states, contemporary politically-heterogenous East Asia, due to '[r]apid economic development, which contributes to the legitimacy and capacity of governments', has nonetheless experienced decline in intrastate conflicts, making it a relatively stable region to cooperate with.[138] ASEAN has played not the last role in this, gradually changing its position from that of opposition towards supranational legislation into the "ASEAN Way" of collective security through intelligence sharing ,especially in the aftermath of the September 2001 benchmark terrorist attacks[139]; this commitment, however, was evident some years before in the ASEAN Declaration on Transnational Crime, outlining principles of fighting transnational crime 'through intelligence sharing, harmonisation of policies and coordination of operations'.[140] Question of cybersecurity has also been raised multiple times on the ASEAN agenda over the last decades: during the 3rd ASEAN Ministerial Meeting on Transnational Crime held on 11 October 2001 in Singapore, ASEAN Ministers responsible for transnational crime agreed to include cybercrime in the Work Programme to Implement the *ASEAN Plan of Action to Combat Transnational Crime*. Almost twelve years later, in September 2013, a SOMTC Working Group on Cybercrime was created.

---

[135] FRANDA, Marcus (2002) *Launching into Cyberspace: Internet Development and Politics in Five World Regions*, London: Lynne Rienner Publishers [pp. 85-86]; cf. SENOR, Daniel Samuel, and SINGER, Saul (2009) *Start-up Nation: The Story of Israel's Economic Miracle*, New York City: Hachette Book Group. Israel, at the same time, is an interesting case study when looking at regulatory policies on encryption. Having sold 10% of global encryption products in 2014, the "cyber-entrepreneurial" state, instead of securing access to the encryption keys or access points, stresses government-private sector collaboration in answering national threats (see further: https://www.lawfareblog.com/how-does-israel-regulate-encryption ; http://www.lexology.com/library/detail.aspx?g=b31fe40f-9564-44cf-b241-bcda18c0fc61)

[136] VOETEN, Erik (2010) 'Regional Judicial Institutions and Economic Cooperation: Lessons for Asia?', *Working Paper Series on Regional Economic Integration No. 65,* available online at: https://aric.adb.org/pdf/workingpaper/WP65_Voeten_Regional_Judicial_Institutions.pdf [p. 7]

[137] KAHLER, Miles (2013) 'The Rise of Emerging Asia: Regional Peace and Global Security', *Working Paper 13-4*, Peterson Institute for International Economics, available online at: http://lea.vitis.uspnet.usp.br/arquivos/the-rise-of-emerging-asia-regional-peace-and-global-security_miles-kahler.pdf [p. 9]

[138] ibid. [p. 2]

[139] BUDD, Darlene (2017) 'Association of Southeast Asian Nations (ASEAN)', in SILANDER, Daniel, WALLACE, Don, and JANZEKOVIC, John (eds) (2017) *International Organizations and the Rise of ISIL,* London: Routledge [pp. 58-61]

[140] ASEAN (1997) *ASEAN Declaration on Transnational Crime,* Manila, December 20 [published online on 4th July 2012], available online at: http://asean.org/?static_post=asean-declaration-on-transnational-crime-manila-20-december-1997 [pp. 60-61]

A potentially boosting factor to the development of overarching cybercrime prosecution enforcement mechanisms between ASEAN, the West and other regions is a new INTERPOL Global Complex of Innovation in Singapore, created with the goal of fostering cybersecurity and countering cybercrime by complementing the shadow operations rooms in Lyon and Buenos Aires in guaranteeing daytime coverage of most of the globe, enhancing INTERPOL's presence in Asia and thereby 'go[ing] beyond the traditional reactive law enforcement model'.[141] Global connection through this executive mechanism might foster cooperation in the judicial realm as well, with a possible spillover effect on the neighbouring state parties to regional organizations (apart from ASEAN, Shanghai Cooperation Organization, Conference on Interaction and Confidence-Building Measures in Asia, etc.). One case concerning the suicide of a sexually-harassed and blackmailed Scottish juvenile Daniel Perry in 2014 demonstrates willingness of the Asian countries to cooperate in a joint investigation, led by the INTERPOL and aided by US Immigration and Customs Enforcement Homeland Security Investigations, UK National Crime Agency, Hong Kong Police Force, Singapore Police Force, and the Philippines National Police Anti-Cybercrime Group.[142] However, the fact that the nature of crime was child sexploitation – a matter condemned equally strongly in different world regions – played a great role in the successful cooperation.

When it comes to more controversial crimes and the prospect of a (even if abstract and non-existent at this point) regional judiciary coming before and on behalf of states, the problem that has to be kept in mind lies in Asian governments' traditional reluctance 'to delegate substantial authority to regional institutions'.[143] Experience of colonialism, non-recognition of Communist regimes (which led to the 'perception that international law is primarily an instrument of political power'[144]) and selectivity of international criminal law after post-WWII trials[145] made Asian countries especially hostile to the idea of supranational judiciary and dominance of the international law, hostility which will take time to dissolve. One exception is, similarly to the GCC dynamic, commercial arbitration, which is on a considerably developed level: worth mentioning are Hong Kong International Arbitration Centre ("HKIAC") and Singapore International Arbitration Court ("SIAC"). Both are party to the 1958 New York Convention on Recognition and Enforcement of Arbitral Awards[146], 'meaning arbitral awards from either jurisdiction are enforceable in 150 different countries', including the ASEAN members.[147] Regional cooperation in prosecution for cyberterrorism, politically-motivated hacking and similar cyberoffences can still largely depend on MLATs and interstate relations. As an example 9though not from the field of cybersecurity), PRC's recent white paper on South China Sea conflict shows the still-preferable bilateral approach of Beijing to resolve the conflicts concerning its national security by posing

---

[141] from the INTERPOL's page for the Global Complex for Innovation: https://www.interpol.int/About-INTERPOL/The-INTERPOL-Global-Complex-for-Innovation

[142] INTERPOL (2014) *INTERPOL-coordinated operation strikes back at 'sextortion' networks*, May 2, available online at: https://www.interpol.int/News-and-media/News/2014/N2014-075

[143] *supra,* note 137 [p. 15]

[144] CHESTERMAN, Simon (2017) 'Asia's Ambivalence About International Law & Institutions: Introduction to Opinio Juris and EJIL:Talk! mini-symposium', *EJIL: Talk!*, January 16, available online at: https://www.ejiltalk.org/asias-ambivalence-about-international-law-institutions-introduction-to-opinio-juris-and-ejiltalk-mini-symposium/

[145] ibid.

[146] see: http://www.arbitration-icca.org/media/0/12125884227980/new_york_convention_of_1958_overview.pdf

[147] CLARKE, Marquise (2014) 'Successfully Resolving Commercial Disputes: An Overview of Arbitration in ASEAN', *ASEAN Briefing,* June 28, available online at: http://www.aseanbriefing.com/news/2016/06/28/asean-arbitration.html

that internationalisation and judicialization of the issue 'will only make it harder to resolve […], and endanger regional peace and stability'[148] – an approach that is characteristic of the overarching cross-border dispute-settlement culture in Asia.

Some developments, nevertheless, can be seen on a domestic scale, such as an interesting example described below, which might lay one foundation stone or serve as a model for further subject-specific (or, rather, crime-specific) regional judicial integration. It comes from the Philippines' Cybercrime Prevention Act[149] which, among other functions, marked the establishment of the Office of Cybercrime within the Department of Justice as the central authority in questions of international mutual assistance and extradition in direct cooperation with the national Cybercrime Investigation and Coordinating Center, responsible for policy coordination and for the design and implementation of the domestic cybersecurity framework under the Office of the President. Originally jurisdiction of the Act, which

> shall lie if any of the elements was committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country, or when by such commission any damage is caused to a natural or juridical person who, at the time the offense was committed, was in the Philippines,

is given to the Regional Trial Court with primary jurisdiction the Act (Chapter V, section 21). Yet here comes one of the most interesting points: the Act specifies that 'there shall be designated special *cybercrime courts* manned by specially trained judges to handle cybercrime cases'[150]; as of May 2017, the Supreme Court has assigned cybercrime-prosecution functions to certain branches of the Regional Trial Courts.[151] The case is meaningful in comparison with the afore-discussed global tribunal in their similar focus on excellence and expertise of the judges in the field, which would require combined legal and IT training, with a special focus on the Intellectual Property Law and 'liaising effectively with computer specialists for the presentation of lengthy and complex evidence'.[152]

3.3.1 Where is China in it?

Within the EU-ASEAN cooperation what we have *not* seen is EU's equal engagement[153] with China, a growing cyberpower, despite the expressed predisposition to joint efforts in securing

---

[148] Ministry of Foreign Affairs of the People's Republic of China, *China's Policies on Asia-Pacific Security Cooperation*, published on 11th January 2017, available online at: http://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1429771.shtml

[149] *Cybercrime Prevention Act of 2012 (Republic Act No. 10175),* adopted by the Second Regular Session of the Fifteenth Congress of the Philippines, 12th September 2012, available online at: http://library.pcw.gov.ph/sites/default/files/RA-10175-BSA.pdf

[150] ibid. (emphasis added)

[151] CANLAS, Jomar (2017) 'SC designates cybercrime courts', *The Manila Times*, May 7, available online at: http://www.manilatimes.net/sc-designates-cybercrime-courts/326021/

[152] SMITH, Russel Gordon, GRABOSKY, Peter Nils, and URBAS, Gregor Frank (2004) 'Sentencing Cybercriminals', in *Cyber Criminals on Trial*, New York: Cambridge University Press [p. 125]

[153] The very fact of China's non-participation in multilateral arrangements and any regional or global systems of regulation (be it the Budapest Convention, APEC's Cross-border Privacy Enforcement Arrangement, or the Asia-Pacific Privacy Authorities) is not surprising per se, in contrast to the numerous bilateral agreements, such as the one with Russia (2015), which reaffirms the 'jurisdiction of the state over the information infrastructure in their territories, as well as that the state has a sovereign right to design and implement the policy in the field of information telecommunication networks, including provision of safety' – see: http://government.ru/media/files/5AMAccs7mSlXgbff1Ua785WwMWcABDJw.pdf [pp. 1-2; translated from Russian by Olesya Dovgalyuk]

cyberspace by China's President Xi Jinping and the head of ChinaEU, Luigi Cambardella.[154] The latter's proposals of altering ENISA's direction during the revision of its strategy to focus on building China-EU cyberspace governance, if taken into account, might present an intriguing case of emerging relations between the two actors in the future, with the possibility of the EU and ASEAN as external mediators for each other's relations with the Asian giant.

When it comes to national legislation, the only state having to-date ruled out a death sentence for a computer crime[155] has always had an advantage of the wide applicability of the existing Penal Law to the variety of cases through judicial interpretation. Subsequent amendments thereof (in a chronological order) filled in the gaps by criminalising illegal intrusion into computer information systems (Article 285) and destruction of computer information systems (Article 286), while *The Management Measures on Computer Virus Prevention* prohibited any unit or individual to create (Article 5) and spread (Article 6), computer viruses, as well as publish false computer viruses epidemic situation to society (Article 7). All-included, while Chinese cyber- and computer-offence-related legislation is non-unified, fragmented in its dispersal among different sources of national law (the penal code, special statutes, legislative and judicial interpretations, and administrative regulations)[156], and thereby sometimes overlapping, it still presents a comprehensive set of binding measures, which can serve as a fundamental common ground for international coordination with foreign law enforcement agencies and judiciary. All this notwithstanding, China has not yet gained much trust from the outside world; one of the roots of the animosity lies in the difference between the epistemic communities of the West and those of China and its like-minded allies (e.g. Russia): a general security-related reason has been its constant striving for the implementation of a partial information blockade by filtering contents, limiting access and blocking numerous sources, thereby creating what was labelled as "Chinternet". The latest example of this dynamic is the Cybersecurity Law (in force on 1st June 2017), which requires businesses, 'network owners, managers, and providers'[157] to disclose their proprietary source code (to prove their defence mechanisms against hacking) and obliges them to store sensitive data and personal information gathered in China within the latter's borders – altogether accelerating China's 'jurisdictional control over content on the internet'.[158] It is barely surprising why Western states are wary of cooperating with such a government, especially in the practice of extradition and in the light of the fact that vulnerability of general users is being largely ignored: objects of the offence (i.e. to be protected) under the Article 285 of the Criminal Law are limited to 'computer information systems of national affairs, construction of national defence, or belonging to the field of top science and technology'[159], reflecting the main diverging point of China (and other

---

[154] ChinaDaily (2017) *EU should deepen cyber security cooperation with China: Digital expert*, March 4, available online at: http://www.chinadaily.com.cn/business/tech/2017-03/04/content_28434805.htm

[155] GITTINGS, John (1998) 'China sentences bank computer hackers to death', *The Guardian*, December 30, available online at: https://www.theguardian.com/world/1998/dec/30/johngittings1

[156] ZHANG, Xiaoyan – Mayer Brown LLP (2017) Data Security and Cybercrime in China, *Lexology*, available online at: http://www.lexology.com/library/detail.aspx?g=6a51305a-eccd-4f3f-a3a4-0b9e21843c19; LI, Xingan (2015) 'Regulation of Cyber Space: An Analysis of Chinese Law on Cyber Crime', *International Journal of Cyber Criminology*, 9(2): 185-204 [p. 203]

[157] WAGNER, Jack (2017) 'China's Cybersecurity Law: What You Need to Know', *The Diplomat,* June 1st, available online at: http://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/

[158] ibid.

[159] *supra*, note 156 (LI) [p. 202]

regional powers, such as Russia) if compared to the West, which is its (neglectful) 'approach to human rights norms and […] norms on protection of intellectual property rights affected by cyber espionage'.[160]

Economic espionage and cybercrimes by non-state actors is another issue causing distrust between China and other states, especially taking into account the diverse nature of the hacking/criminal groups, and the semi-clear endorsement from the government (as opposed to the common depictions of a centralised offensive cyber-policy). For instance, the fact that intelligence gathered through the cyber espionage of the "Advanced Persistent Threat-1" ("APT1") – which in itself is capable of sustaining unusually long-term and extensive for a non-state entity espionage campaigns (mostly against the US firms, but also in other states such as South Africa, Switzerland, the UK, Japan, etc.) – is reflected in the official PRC Cyber strategy (targeted industries 'match [those] China has identified as strategic to their growth, including four of the seven strategic emerging industries that China identified in its 12th Five Year Plan') is given by Mandiant as one of the arguments for the strong likelihood of its identicality with the Unit 61398 (part of People's Liberation Army), as well as the PRC government's awareness of the group's existence and sponsorship of their operations.[161] While espionage itself is a more or less normalised state practice, stealing and using intellectual property – inappropriate and unacceptable for the US – for China is '[t]he only way [to] sustain [its] economic growth' and thereby maintain internal political stability.[162]

However, full-scale open confrontation is usually avoided: China is cautious not to compromise collaboration channels with the West – especially in the face of the rising India's cyberpower, its growing cooperation with the US and South-Asian states (despite traditional rivalry with Pakistan)[163], – beneficial for maximising trade opportunities and economic interaction. To show its global standing, China actively participates in the global institutions[164] to soften harsh edges and accommodate the two sides' interpretation of individual rights online, as well as to reassure responsible governments by introducing mechanisms making the agreement violation-proof from interference in national sovereignty. Shanghai Cooperation Organization, whose official languages are Chinese and Russian only, is a perfect regional forum for China and Russia to secure regional security community, solidifying local support for their strategy, and only then challenging Western frameworks (presented by the already-mentioned Budapest Convention) through international norm-building, as they did in the UN.[165]

---

[160] AUSTIN, Gregory (2016) 'International Legal Norms in Cyberspace: Evolution of China's National Security Motivations', in OSULA, Anna-Maria, and RÕIGAS, Henry (eds) *International Cyber Norms: Legal, Policy & Industry Perspectives,* NATO CCD COE Publications [p. 173]

[161] Mandiant (2013) *APT1: Exposing One of China's Cyber Espionage Units*, available online at: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf

[162] Larry CLINTON (ISA's CEO) quoted in CHABROW, Eric (2015) 'Cyber Lexicon: U.S., China Speak Different Languages: Preparing for U.S.-China White House Summit', *BankInfoSecurity*, September 14, available online at: http://www.bankinfosecurity.com/blogs/cyber-lexicon-us-china-speak-different-languages-p-1936

[163] KIRAN, R. Bhanu Krishna (2012) 'India's War on Terrorism and International Cooperation', *Society for the Study of Peace and Conflict*, available online at: http://www.sspconline.org/opinion/IndiasWaronTerrorismandInternationalCooperation_13072012

[164] ITU Secretary-General Houlin Zhao; Director-General of the United Nations Industrial Development Organization Li Yong; etc.

[165] AUSTIN presents a relevant for this case differentiation between types of international norm-forming, which 'can be one that is universally agreed (and therefore of universal application), or one limited to a group of consenting states (applying only to them)' – see *supra,* note 160 [p. 172]

3.4 Europe & Transatlantic cooperation

In the judicial realm, Europe is a highly integrated region. One of the reasons behind it has been close communication between national and regional courts, exemplified among others by the fact that, facing uncertainties in the interpretation of laws,

> national courts may engage in a judicial dialogue with the CJEU through the preliminary reference procedure. [The fact that] [i]n this process national courts, seised of a case with an EU legal element, may (or, if a last instance court, must) refer questions to the CJEU on the interpretation of EU law, the answers to which they are bound to apply in the case before them,[166]

over the years strengthened the rule of law through the binding of the parties to the CJEU decisions (Article 46(1) of the Convention), and contextualised integration of the Union. Zooming into the cybercrime aspect of common legislation, Europe as of today is considered one of the most forward-standing regions. One of the earliest legal responses to the cybersecurity threats in the EU was the adoption of the 2005/222/JHA *Act On Attacks against Information Systems*, which set as its objective intraregional harmonisation of law and 'the greatest possible police and judicial cooperation in the area of criminal offences related to attacks against information systems'.[167] By outlining – although roughly – penalties for cyber and computer-related crimes, as well as criteria for jurisdiction in prosecution, it partially fulfilled its initial goal and thereby has served as a ground to all further projects and frameworks (such as *e-CODEX Project for cross border e-Justice,* and so forth). The recent *Directive on network and information systems* (NIS Directive)[168] aims to further foster 'the development of principles for European cyber-crisis cooperation' and secure the online environment for Single Digital Market by addressing the fragmented nature of the response to cyberthreats due to the uneven level of preparedness across the Member States.[169]

European networks of cybercrime prevention in the legislative domain are also some of the most far-reaching with regards to the interregional cooperation, effectively extending beyond the union's borders, reaching out all over the world to the states member to East-Asian, African, Eastern-European and Central Asian, and Inter-American regional organizations, not only bilaterally increasing cybersecurity capabilities, but also, importantly, creating judicial network and encouraging international cooperation, specifically, under the Council of Europe Convention on Cybercrime ("Budapest Convention"). In March 2017 the Cybercrime Programme Office of the Council of Europe ("C-PROC"), for instance, provided 'support on legislation, judicial and law enforcement training, institution building, public/private and

---

[166] *supra,* note 35

[167] *Council of the European Union Framework Decision 2005/222/JHA of 24 February 2005 on attacks against information systems*, available online at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32005F0222&from=EN

[168] *Directive (EU) 2016/1148 Of The European Parliament And Of The Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union*, available online at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN

[169] ibid.

international cooperation' to numerous non-members of the Union[170], as well as collaborated with some MENA states on the new CyberSouth project[171] and continued their efforts in the GLACY+ (2016-2020) Project with Mauritius, Morocco, Senegal, South Africa, Sri Lanka and Tonga. Some of the agreements were less successful than others: for example, so-called *Safe Harbour* data protection agreement between the US and the EU failed to reach its objectives, being declared invalid by CJEU after a case regarding Facebook data protection failure was filed following Snowden's revelations.[172] Still, mutual legal assistance between the EU and the US remains one of the strongest partnerships in 'cross-border law enforcement and intelligence, including counter-terrorism'[173], despite differences in institutional frameworks. Formal relationship dates back to the 1995 *New Transatlantic Agenda* on cooperation in Justice and Home Affairs, and since then it (although not evenly, but overall) gradually strengthened on both bilateral and multilateral levels. In addition to network-building activities managed by the US-EU Working Group on Cyber-Security, such as regular visits by the US representatives to Europol, trainings and awareness campaigns, and joint actions by law enforcement and judicial agencies are undertaken. On the practical side of law enforcement, worth mentioning is a successful global *Operation Onymous* against black-net markets on TOR (a free network anonymising IP addresses), coordinated collectively by European (Europol's Cybercrime Centre (EC3); Eurojust) and US institutions (the FBI; Immigration and Customs Enforcement (ICE); Homeland Security Investigations (HSI)). Results speak for themselves:

> '17 arrests of vendors and administrators running these online marketplaces[;] […]more than 410 hidden services […] taken down. In addition, bitcoins worth approximately USD 1 million, EUR 180 000 euro in cash, drugs, gold and silver were seized. The dark market Silk Road 2.0 was taken down […] and the operator was arrested'.[174]

---

[170] Albania, Armenia, Azerbaijan, Belarus, Bosnia and Herzegovina, Dominican Republic, Georgia, Ghana, Guatemala, Kosovo, Mauritius, Moldova (Republic of), Montenegro, Morocco, Panama, Philippines, Senegal, Serbia, Sri Lanka, "The former Yugoslav Republic of Macedonia", Tonga, Turkey, and Ukraine (from: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680704eb4, p. 1)

[171] Council of Europe (2017) *Cybercrime@CoE Update*, available online at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680704eb4

[172] This followed *Schrems* case, where Austrian plaintiff's complaints about personal data protection to Facebook Ireland and Data Protection Commissioner were rejected on the grounds that as a national supervisory authority, it has no duty under *Safe Harbour* agreement (between the US and EU with compliance to the *EU Data Protection Directive 95/46/EC*) to investigate adequacy of the third country's data protection practices in the transatlantic data flows. CJEU, which was requested for a clarification of the case by the Irish High Court, ruled upon the examination of the *Safe Harbour*

> '…that there was no decision on US laws or treaties that would limit this interference (¶88), provide effective legal protection (¶89), or provide individuals with legal remedies', despite the fact that 'processing of [the EU citizens'] personal data [by the US authorities] went beyond the scope of what was necessary and proportionate for reasons of national security' (https://ccdcoe.org/top-eu-court-finds-eu-us-personal-data-transfers-not-safe-enough.html).

It also ruled out that national authorities under Art. 3(1) of the Directive are denied powers to ensure compliance with Art. 25(6) (https://www.dataprotection.ie/docs/EU-Directive-95-46-EC-Chapters-3-to-7-Final-Provisions/94.htm) and, as a consequence, declared the whole *Safe Harbour* agreement and principles invalid. Developments in the new *EU-US Privacy Shield* which places 'stronger obligations on U.S. companies to protect Europeans' personal data' (http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf), to overcome the issues that brought its predecessor down remain to be closely followed. (*Judicial Redress Act* allowing foreign citizens in European countries to sue the United States for unlawful disclosure of personal information, passed later in the US Congress, somewhat softened the transatlantic divide on the government's invasion of individuals' privacy).

[173] CÎRLIG, Carmen-Cristina (2016) *EU-US cooperation in Justice and Home Affairs – an overview*, European Parliamentary Research Service, available online at: http://www.europarl.europa.eu/RegData/etudes/BRIE/2016/580892/EPRS_BRI(2016)580892_EN.pdf [p. 2]

[174] EUROPOL (2014) 'Global action against dark Markets on TOR network', *Press Release*, November 7, available online at: https://www.europol.europa.eu/newsroom/news/global-action-against-dark-markets-tor-network

Further harmonization between Europe and America(s), however, 'is essential to surmount the growing substantive and procedural barriers to cross-border Internet-related tort litigation'.[175]

Within Europe itself, the problem paradoxically lies in the area which also makes it the strongest: it is the elaborate institutional framework, incorporating numerous agencies each specialising in a single aspect of cybersecurity and cybercrime response (trade-related, privacy and data protection, anti-child pornography etc.). Although it is true that '[m]anaging cyber-space and digital technologies cannot be forced into one single form, nor can one actor or agency be responsible for developing anticipatory governance and practices'[176], too diverse diffusion of powers in this nodal model of governance can lead to another extreme, resulting in considerable delays in specifically institutional response. For instance, while acknowledging the importance of oversight and deliberation by different agencies to ensure high quality and objectivity of the decisions made, different perspectives of the Council of the EU and European Parliament regarding the aforementioned NIS Directive took around one-and-a-half years[177] of trilogue meetings[178] and talks to finalise the initiative.

4. The gap between the Public and the Private

Several difficulties, not only at the inter-states level, permeate the effective data-sharing cooperation to inform the investigation and prosecution processes. While the privatisation of critical infrastructure by non-state entities '[could be] economically beneficial to the state, freeing up capital and drawing more heavily on the efficiencies and business practices of the private sector', it also means that there have to be mechanisms to secure compliance of private institutions[179], which is often a problematic process as evident from internet giants' protectionist stance in relation to their clients' and users' data. It is (expectedly) most observable in the states where the gap between the official public institutions and the private sector is deep, e.g. the UK or the US. The latter especially faces the contradictions of the so-called 'third-party doctrine [which claims] that individuals do not have Fourth Amendment protections in information that has been shared with other people or organizations', as seen in the *United States v Jones,* and *Riley v California* cases.[180]

---

[175] *supra*, note 2 [p. 157]; in the economic realm of data-protection a proposal of a 'Transatlantic Charter for Data Security and Mobility' to address uncertainties around conflicting jurisdictions for transatlantic start-ups, firms and banks has been made – see SMART: https://www.chathamhouse.org/sites/files/chathamhouse/publications/research/2017-06-28-regulating-data-economic-growth.pdf

[176] MUNK, Tine Højsgaard (2015) 'Cyber-security in the European Region: Anticipatory Governance and Practices', DPhil Thesis, School of Law at the University of Manchester (UK), available online at: https://www.research.manchester.ac.uk/portal/files/54570851/FULL_TEXT.PDF [p. 67]

[177] The first trilogy meeting took place on 27 November 2014, and the final text being approved by the Council on 26 May 2016 and the Parliament on 6 July 2016

[178] Trilogues/trialogues are types of meetings in the EU attended by the Council (of the EU), the Parliament and the Commission.

[179] CARR, Madeline (2016) 'Public–private partnerships in national cyber-security strategies', *International Affairs*, 92(1): 43–62, retrievable from: https://www.chathamhouse.org/publication/ia/public-private-partnerships-national-cyber-security-strategies [pp. 43; 48]

[180] Law Enforcement Cyber Center (2015) *U.S. Supreme Court Cases: Discussion of Recent Supreme Court Jurisprudence*, available online at: http://www.iacpcybercenter.org/prosecutors/case-law/

This controversy can be explained by different perceptions of cyberthreats (as both executed in the cyberspace or in the physical reality with the help of technological devices) in private and public sectors, where the former 'regards cyber-security challenges as financial and reputational [in the light of the potential loss of status if failures are exposed to competitors in the field – added by us] — not as a common public good, which is how governments regard national cyber security'[181]; when the situation does not allow for both to harmoniously cooperate against the threats, the denial of responsibility is observable.[182] These difficulties on a global level are exacerbated by heterogenous national governments' positions in cyberdefence power-sharing policies on the public-private scale, with the contrasting comparative examples of the China's state-centered cybersecurity and the US diffused privatisation.

So far Western liberal multi-stakeholder model has proven comparatively successful, corresponding to the complex pattern of ownership and governance of the domains and computer systems – with a reservation, however, that the multistakeholder model is not a consensual promotion of the US corporate interests by the group of insiders, an idea also re-confirmed at the latest World Summit on Information Society (WSIS) Forum in June 2017.[183] At the same time, it is crucial to remember that assignment of the 'responsibility for the future of the Internet to a broader community including governments, the private sector, civil society and technical experts'[184] is to be done in a differentiated and proportional way, with some actors – e.g. government and security experts, and business owners – having greater responsibilities, since cyberwarfare, if a reality, will be a war of few highly-skilled individuals, whole populations being victims of its consequences. To be addressed, it will not only need a general good "communal cyber-hygiene", but also timely and professional countermeasures by equally skilled experts. As the absolute minimum, demands for a less US-centric multistakeholder system[185], manifested in the system of the Internet Corporation for Assigned Names and Numbers (ICANN), have to be addressed in the design of a shared intergovernmental platform to be used on a supranational level. The transition can be further done via different models, but its necessity is clear: technicians and engineers who created internet and ICT with the idea of an open rather than secure system have to show a more active coordination with the legal experts and the private sector – responsible before its clients for the confident information –, for all the stakeholders to be proportionately engaged in cybergovernance.

The last difficulty associated with the diffusion of power to highlight in this article (which by no means exhausts the list of dangers associated with cyberspace and ICT) is the seeming inevitability of imbalances and shifts, with 'temporarily increased entanglement [of some states] with [certain institutions of governance] because they or their nationals serve in a

---

[181] *supra,* note 179 [p. 55]

[182] see, for example: https://www.theguardian.com/technology/2016/feb/17/inside-the-fbis-encryption-battle-with-apple

[183] POWERS, Shawn M., and JABLONSKI, Michael (2015) *The Real Cyber War: The Political Economy of Internet Freedom,* Champaign: University of Illinois Press [p.136]. For the outcomes of the WSIS 2017 Forum see: https://www.itu.int/en/itu-wsis/Documents/wf17/WSISForum2017_ForumTrackOutcomes.pdf

[184] ibid. (POWERS)

[185] Recently, US passed the governance of Internet domain names and numbers on to ICANN via the IANA process, which as a model of transition into a multi-stakeholder governance was not without drawbacks – see: http://www.tandfonline.com/doi/pdf/10.1080/23738871.2016.1227866?needAccess=true

position of authority'[186], and detachment when this authority ceases to dictate the tone and content of agenda. This creates fragmentation, which arguably leads to the afore-analysed regionalism and sub-regionalism in adjudication as well. And while judicial independence 'from external – particularly political – pressures is safeguarded by various institutional means'[187], the broader environment within which the Courts and Tribunals operate, coupled with their financial dependence[188], inevitably makes them targets of politicisation. In this sense even second-generation trade organisations, when involved into the process of prosecution for cybercrimes and thus empowered with mandates on the questions of collective security, might seriously corrupt the institute of judiciary, undermining its perceived neutral authority (sometimes precisely through offering State Parties certain *economic* benefits), and therefore have to be handled carefully.

[186] VOETEN, Erik (2014) 'Does participation in international organizations increase cooperation?', *Review of International Organizations*, 9: 285-308, available online from: http://link.springer.com/article/10.1007/s11558-013-9176-y [p. 285]

[187] DE BAERE, Geert, CHANÉ, Anna-Luise, and WOUTERS, Jan (2015) 'Assessing the contribution of the international judiciary to the rule of law: elements of a roadmap' – *Working Paper No. 157*, available online at: https://ghum.kuleuven.be/ggs/wp157-debaere-chane-wouters.pdf [p. 12]

[188] for example, the then-President of the ICJ Stephen Myron Schwebel identified this through the recognition that '[t]he Registry, and the budget of the Court, essentially were designed for an era when the Court had few, not many, cases on its docket' – see United Nations (2002) *Yearbook of the International Court of Justice*, vol. 54 (1999-2000), The Hague: United Nations Publications [p. 286].

CONCLUSIONS: LAYING THE FOUNDATION STONE

The Internet, or Cyberspace, has been transformed from what arguably was a no man's land, where no laws were seen to apply, to something that more realistically can be described as an "every man's land", where the laws of all states apply at the same time [189]

Whether fragmentation in the form of cooperative regional/national judiciaries with the statutes/treaties "boosted" by cybercrime regulations would bring about more effective changes if compared to the establishment of a centrally-unified tribunal, remains a rhetorical question, an answer to which might rather be found on a scale between these two mutually non-exclusive options.[190] Only practical actions and time will show which solution works better. At this point the design of such actions should be partially handed over to experts (akin to the group which produced both versions of the *Tallinn Manual*) to be scrutinised with the afore-discussed geographical, legal and cultural disparities and incompatibilities in mind.

Certain final remarks about these have to be made.

1. Cybersecurity vs. Cyberdemocracy?

As 'ICT[s] reinforce rather than reverse embedded participatory inequalities in a global context, and fail to substantially increase transparency and accountability'[191], the fiercely defended online privacy, while providing space for greater anonymous expression, can in some occasions only slow down or impede in any other way identification of potential criminals, thereby pushing states into the murky relations with intelligence agencies. Since harmonious convergence of legal systems has not proven evenly successful so far, cyber governance in the form of "cyberborders" promoted in the SCO *Suggested Code of Conduct* can be implemented to prevent or, at least, minimise the opportunities and regulate the platforms for transitional e-crimes. These 'cyberborders could be drawn and are already drawn, either through the voluntary blocking actions of foreign providers[,] by filtering foreign content through ISPs'[192], or restricted access for foreigners, for example – all despite fierce lobbying by some civil society bodies for a transparent and democratic e-governance.[193] This measure, however, has to be taken as a short-term response only. Further adjudication and harmonisation is absolutely necessary if we want to have the benefits of transnational communication that we currently enjoy and simultaneously make the environment for this exchange safer.

---

[189] SVANTESSON, Dan Jerker Börje (2007) *Private International Law and the Internet* (1st edition), Alphen aan den Rijn: Kluwer Law International BV [p. 2]

[190] This might come with all the concomitant challenges of conflicts regarding jurisdiction 'and a danger that regional courts might be inspired by regional legal conceptions to such an extent that their decisions might prejudice the future unity of the law of nations in respect of matters regarding which uniform rules of world-wide validity are desirable' (SLOMANSON, William R. (2010) *Fundamental Perspectives on International Law*, Wadsworth: Cengage Learning, p. 437).

[191] SÉNIT, Carole-Anne, KALFAGIANNI, Agni, and BIERMANN, Frank (2016) 'Cyberdemocracy? Information and Communication Technologies in Civil Society Consultations for Sustainable Development', *Global Governance,* 22: 533-554, available online at: http://journals.rienner.com/doi/pdf/10.5555/1075-2846.22.4.533

[192] *supra,* note 62

[193] For example, Just Net Coalition in their *Delhi Declaration for a Just and Equitable Internet* called for the replacement of the '[c]urrent control by one country of the DNS/root zone [with] a new transparent, accountable and internationally representative institution responsible for the oversight of critical Internet resource management functions' – see: https://justnetcoalition.org/delhi-declaration (point 23)

2. Homogenising basic concepts of international cybersecurity legislation

Whichever type of judicial action is taken in a specific case – global supranational, or regional/international (through bilateral and multilateral arrangements), – common legal concepts[194] in cybersecurity matters are a crucial milestone in ensuring grounds for cooperation, creating a common reference point for law enforcement. And it is easy to see why: explaining it through CREEKMAN's example of the United States and China, '[b]oth […] would benefit more from a multilateral agreement rather than a bilateral agreement' on mutual legal assistance, into which neither would probably be willing to enter due to substantive differences in judicial systems.[195] '[R]egional or bilateral cybercrime instruments […] create a cooperation cluster that is unable to address the global nature of cybercrime'[196], and currently existing MLAs are not sufficient in addressing transjurisdictional crimes, which often results in numerous diverging approaches, taken unilaterally by different governments. As rightly noted, 'for a crime to be prosecuted by an international tribunal it should be recognised as serious and international under customary international law'; it should become a convention.[197] As an exemplar pre-requisite, or the program-minimum, 'at least [Articles 2-9] in the substantive criminal law section' of the 2001 Council of Europe *Convention on Cybercrime*[198] could be incorporated into all national legislations as they 'identify broad principles that form opinio juris and thereby can build a foundation for international obligations'.[199] The Convention itself, in the light of its sixteen-year life, is outdated and has to be updated to reflect the technological advancements and the new methods of cyber attacks and types of cyber crimes, including the challenges of cloud computing and multi-jurisdictional crimes[200]; however, it serves its (symbolic?) purpose for the time-being, and shows the potential to serve as a foundation for the global treaty as more and more states[201] sign and ratify it (Tonga being the latest state to do so this year).[202]

Just as Constitutions in the newly-established nations have as one of their purposes recognition by the international community of states' independence and self-sufficiency[203], the

---

[194] see *supra*, note 2

[195] *supra,* note 57 (CREEKMAN) [p. 676]

[196] TAMARKIN, Eric M. (2015) *The AU's cybercrime response: A positive start, but substantial challenges ahead*, Policy Brief No. 73, Institute for Security Studies, available online at: https://issafrica.s3.amazonaws.com/site/uploads/PolBrief73_cybercrime.pdf [p. 6]

[197] *supra,* note 112

[198] Council of Europe (2001) *Convention on Cybercrime*, European Treaty Series - No. 185, Budapest, November 23, available online at: https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561. As of July 31, 2017, fifty-three states are parties to the treaty; with the signature of San Marino, forty-six out of forty-seven members of the Council of Europe have either signed or ratified the Convention (https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680704eb4, p. 2)

[199] SHACKELFORD, Scott J., RUSSELL, Scott, and KUEHN, Andreas (2016) 'Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors', *Chicago Journal of International Law*, 17(1), available online at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil [p. 7]

[200] *supra,* note 44 [pp. 6 & 10]

[201] Nonetheless, there are still reluctant areas of the world, unhappy with, among other things, its Art. 32 – see: http://thediplomat.com/2017/08/time-for-asean-to-get-serious-about-cyber-crime/.

[202] Council of Europe (2017) *Tonga joins the Budapest Convention on Cybercrime*, May 9, available online at: http://www.coe.int/bg/web/portal/-/tonga-joins-the-budapest-convention-on-cybercrime

[203] RESNIK, Judith (2015) 'Constructing the "Foreign": American Law's Relationship to Non-Domestic Sources', in ANDENAS, Mads, and FAIRGRIEVE, Duncan (eds) *Courts and Comparative Law,* Oxford: Oxford University Press, pp. 437-471

accession to and ratification of global treaties (and participation in associated institutions of both judicial and non-judicial character), if performed by several strongest global actors, can give any such convention or statute a vital endorsement. Further interaction in such institutions would hopefully socialise governments into identifying with their goals, as 'acquiring a position of authority in an [International Organization] can make states more willing to […] adopt domestic legislation that changes the penal code [and] ratify legally binding treaties'[204], in a mixed legalisation process where state preferences are politically "uploaded" to a supranational organization and subsequently "downloaded" from the latter to the state level in the form of legal stances. Additional actions should be taken to make '[t]he costs of leaving [both normatively and financially] too high to consider withdrawal from the respective judicial bodies as a valid option'[205], such as – for example – denied access to a potential common database. Thereby, even countries reluctant to be bound by foreign legislation, such as e.g. Russia and the US (the former raising 'concerns that [law enforcement agents] might acquire powers across national boundaries without consent from the local authorities'[206], the latter insisting on its own individuated legal identity), require consideration of external sources of law and thus can be encouraged to cooperate with the international legal authorities. And to ensure that these 'states are not [relying] on domestic law to justify non-compliance with their international obligation', unified international principles of interpretation should be designed simultaneously in a way that 'after their entry into domestic legal systems, international rights or obligations are still to be applied as international law rather than domestic law'.[207] Russia – initially (2011) with China, Tajikistan, and Uzbekistan, later (2015) joined by Kazakhstan and Kyrgyzstan – has shown persistent pursuit of designing an alternative (and more friendly to the values of non-interference and national sovereignty) international anti-cybercrime convention, as seen from the attempts to promote the *Code of Conduct* in UNSC which could replace the Budapest Convention. The outcomes are yet to be seen, but the project has already caused criticisms for its anti-Western sentiment,[208] although in the more assertive tone about protection of state sovereignty it can be seen following the UN GGE conclusion from the *UNGA A/70/174 Report* that:

> sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the

---

[204] *supra,* note 186 [pp. 285; 289; 306]

[205] *supra,* note 187 [p. 14]

[206] PAWLAK, Patryk (2011) 'The EU-US Security and Justice Agenda in Action', *European Union Institute for Security Studies Chaillot Papers*, available online at: http://www.iss.europa.eu/uploads/media/cp127_EU-US_security_justice_agenda.pdf [p. 43]. Another interesting reference for understanding the logic and preferences of Russia, China and some (mostly supporters of Russia-led regional institutions and generally Russian allies) CIS states, is the GA letter A/66/359, submitted by Russia, Tajikistan, China and Uzbekistan to the Secretary-General: https://ccdcoe.org/sites/default/files/documents/UN-110912-CodeOfConduct_0.pdf

[207] NOLLKAEMPER, P. André (2016) 'Grounds for the Application of International Rules of Interpretation in National Courts', in AUST, Helmut Philipp, and NOLTE, Georg (eds) *The Interpretation of International Law by Domestic Courts: Uniformity, Diversity, Convergence,* Oxford: Oxford University Press [pp. 38 & 42]

[208] Russia Today (2014) 'Russia prepares new UN anti-cybercrime convention – report', April 14, available online at: https://www.rt.com/politics/384728-russia-has-prepared-new-international/; Western mistrust continues despite the fact that the controversial term "information weapons" (which might be interpreted with regards to any application such as Twitter or Facebook, thus threatening freedom of expression and flow of information online, fiercely advocated by the Western governments) was removed from the 2015 version of the draft *Code of Conduct*, and substituted with a more vague wording – https://ccdcoe.org/updated-draft-code-conduct-distributed-united-nations-whats-new.html

> purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States,

together with humanity, necessity, proportionality and distinction, are basic IL principles for the State use of ICT.[209] On the other hand, concerns raised by the West are often related to individuals' 'general access to the internet (or digitalised access to information) […] as protected by the universal human right to seek, receive and impart information through any media (see Article 19(1) of the International Covenant on Civil and Political Rights of 1966, Article 10(1) of the European Convention on Human Rights of 1950)'[210], which have frequently been subject to government oppression and which the *Code of Conduct* overlooks with a deliberately loose language.

The most recent call for an international convention came from the private sector under the proposal of the so-called Digital Geneva Convention, shifting focus back on the history of the Internet and to the fact that 'cyberspace [has been primarily] produced, operated, managed and secured by the private sector'; the governments came onto the arena much later to 'play all sorts of critical roles, but the reality is that the targets in this new battle – from submarine cables to datacenters, servers, laptops and smartphones – in fact are private property owned by civilians'.[211] For this reason, alluding to the existent 1949 Geneva Conventions protecting civilians during the wartime, and building on the precedents in achieving consensus on ethical use of cyberspace in the Group of Governmental Experts (GGE), G20 and various bilateral agreements, Microsoft suggested similar restrictions on state actions (i.e. hacking) in cyberspace which have the potential of harming peaceful civilians as in the physical one. The question of non-state actors, as in the case of the International Humanitarian Law, remains problematic. Indeed, the modernity of legal frameworks like IHL and IHRL is challenged, especially when it comes to applying the "Just War Theory" and its principles of "lawful" aggression, discrimination, proportionality, attribution, and non-deception. What is unclear is '*when* a cyberincident becomes an attack' as well as 'to what extent might cyberattacks count as perfidy and therefore be illegal', but also 'how discriminatory cyberwarfare can be', how to reach an international treaty able to make attribution work by agreeing that 'cyberattacks should carry a digital signature'[212], and if cyberspace 'really deserves to be treated as an independent realm of war'.[213]

In the long-term perspective, if successful in addressing the aforementioned controversies, shared legislation – in whatever shape it comes, but which necessarily includes both penal and procedural law[214] – could create favourable conditions for closer technological

---

[209] UN General Assembly (2015) *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security: Note by the Secretary-General A/70/150,* available online at: http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [pp. 12-13]

[210] *supra,* note 58 [p. 163]

[211] SMITH, Brad (2017) 'The need for a Digital Geneva Convention', *Microsoft Blog*, February 14, available online at: https://blogs.microsoft.com/on-the-issues/2017/02/14/need-digital-geneva-convention/#sm.0000f9vglriq9dtqvi6270mu0w84g

[212] LIN, Patrick, ALLHOFF, Fritz, and ABNEY, Keith (2014) 'Is Warfare the Right Frame for the Cyber Debate?', in FLORIDI, Luciano, and TADDEO, Mariarosaria (eds) *The Ethics of Information Warfare*, Berlin: Springer, pp. 39-59 [pp. 41-43, original emphasis]

[213] MORAN, Daniel (2010) 'Geography and Strategy', in BAYLIS, John, WIRTZ, James J., and GRAY, Colin S. (eds) *Strategy in the Contemporary World: An introduction to Strategic Studies* (third edition), Oxford: Oxford University Press, pp. 124-140 [p. 138]

[214] *supra,* note 105 [p. 320]

cooperation both within and between private and public sectors: governments, international organisations and the stakeholder community of ICT companies.[215] This would enable global community to effectively respond to a technological failure or a 'cybergeddon', which is a very likely cause of a global ICT sector turmoil and which requires measures akin to those employed when recovering from major traditional cataclysms.[216]

While trust is a key element in achieving a elementary global consensus, without a strong executive apparatus to oversee states' compliance it is likely to be violated; and in the case of a would-be global judicial body, we would risk falling into the pits of purely symbolic institutionalism, where its "parliamentarization" would 'reinforce intergovernmentalism'.[217] Similarly, lacking enforceable mutual legal assistance agreements, as mentioned above, result in non-compliance and create safe havens for cybercriminals. Better mechanisms of international cyberlaw enforcement should be put in place, as INTERPOL (for instance) is often powerless once state sponsorship of – or support for – cyberattacks is obvious.[218]

Ultimately, in an international legal system which rests on the principles of liberal federalism[219], governance of the cyberspace – by far more anarchic and disordered than the world in the eyes of the realist theory supporters – is a challenge that few would accept. Thus for 'the emergence of a transnational legal order there is a long way to travel'.[220] Some, relying on research, claim that 'public and private regulators are mainly complementary rather than alternatives'[221]; others – that multitude of actors from different sectors only obstructs a cohesive policy. It is the opinion of the authors, however, that, even if the former statement does not always stand for the truth, combined efforts are the only viable option for the balanced cybergovernance. For it to be successful, what has to be accepted and enshrined into the attitude of the stakeholders (especially in the private sector) is that cybersecurity is not impeding or slowing innovation: rather, it is, although not safeguarding against all the pitfalls and mistakes, definitely making their effects less severe and costly. And to succeed in doing so we need 'to look beyond law books, case papers and settled law' to provide justice 'by experiments and by putting innovative ideas into practice'[222] and avoiding duplication of effort, since cybercrimes must be analysed efficiently 'in a temporal context as the technology evolves'.[223]

---

[215] TIIRMAA-KLAAR, Heli (2011) *Cybersecurity threats and responses at global, nation-state, industry and individual levels*, available online at: http://www.sciencespo.fr/ceri/sites/sciencespo.fr.ceri/files/art_htk.pdf [p. 4]

[216] ibid.

[217] *supra,* note 80 [p. 13]

[218] SCHJØLBERG, Stein (2016) *Geneva Declaration on Cyberspace,* available online at: http://www.cybercrimelaw.net/documents/Geneva_Declaration_2016.pdf [p. 11]

[219] *supra,* note 203 [p. 437]

[220] *supra*, note 28 [p. 40]

[221] CAFAGGI, Fabrizio (2014) 'A comparative analysis of transnational private regulation: legitimacy, quality, effectiveness and enforcement', *Comparative Report in the framework of the Project 'Private Transnational Regulatory Regimes - Constitutional Foundations and Governance Design'*, available online at: https://ec.europa.eu/digital-single-market/sites/digital-agenda/files/discussions/HIIL%20Comparative%20Report_final%20june.pdf [p. 70]

[222] The Times of India (2016) 'Special courts needed for cases of cyber crime', September 19, available online at: http://timesofindia.indiatimes.com/city/ahmedabad/Special-courts-needed-for-cases-of-cyber-crime/articleshow/54400724.cms

[223] AWAN, Imran (2014) 'Debating the term cyber-terrorism: issues and problems', *Internet Journal of Criminology*, available online from: https://pdfs.semanticscholar.org/1806/6b03bef29209009b55bfd6301f88a0e0f949.pdf?_ga=2.155224251.1203613720.1503162643-246278333.1503162643 [p. 9]

A BRIEF PROPOSED SELECTION OF FURTHER READINGS

ALEXANDER, Yonah, and SWETNAM, Michael S. (1999) (eds) *Cyber Terrorism and Information Warfare: IV. Research and Development Roadmaps*, Dobbs Ferry (New York): Oceana Publications [pp. 303-304]

ALEXANDER, Yonah, and SWETNAM, Michael S. (1999) (eds) *Cyber Terrorism and Information Warfare: II. U.S. Executive and Congressional Perspectives*, Dobbs Ferry (New York): Oceana Publications [pp. 1-75 and 485-513]

ALEXANDER, Yonah, and SWETNAM, Michael S. (1999) (eds) *Cyber Terrorism and Information Warfare: III. Critical Infrastructure Protection Issues*, Dobbs Ferry (New York): Oceana Publications [pp. 393-429]

ALEXANDER, Yonah, and SWETNAM, Michael S. (1999) (eds) *Cyber Terrorism and Information Warfare: I. Assessment of Challenges*, Dobbs Ferry (New York): Oceana Publications [pp. 221-225]

ALTER, Karen J., (2012) *The Multiple Roles of International Courts and Tribunals: Enforcement, Dispute Settlement, Constitutional and Administrative Review*, available online at: http://scholarlycommons.law.northwestern.edu/facultyworkingpapers/212

AWAN, Imran, and BLAKEMORE, Brian (2012) (eds) *Policing Cyber Hate, Cyber Threats and Cyber Terrorism*, Abingdon-on-Thames: Routledge

BIANCHI, Andrea, and NAQVI, Yasmin (2004) *Enforcing International Law Norms Against Terrorism*, London: Hart Publishing

BOISSON DE CHAZOURNES, Laurence (2017) *Interactions between Regional and Universal Organizations: A Legal Perspective*, Nijhoff: Brill

BOISTER, Neil (2003)'"Transnational Criminal Law"?', *European Journal of International Law*, 14(5): 953-976

Brandeis Institute for International Judges (2016) *The Authority of International Courts and Tribunals: Challenges and Prospects*, available online at: http://www.brandeis.edu/ethics/pdfs/internationaljustice/biij/BIIJ2016.pdf

BROADHURST, Roderic, GRABOSKY, Peter Nils, ALAZAB, Mamoun, and CHON, Steve (2014) 'Organizations and Cyber crime: An Analysis of the Nature of Groups engaged in Cyber Crime', *International Journal of Cyber Criminology*, 8(1): 1-20

BROWN, Cameron S. D. (2015) 'Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice', *International Journal of Cyber Criminology*, 9(1): 55-119

BROWNSWORD, Roger, and YEUNG, Karen (2008) (eds) *Regulating Technologies: Legal Futures, Regulatory Frames and Technological Fixes*, Oxford: Hart Publishing [especially chapters 13, by Andrew Douglas MURRAY, and 17, by Michael Donald KIRBY]

BUCHAN, Russell, and TSAGOURIAS, Nikolaos K. (2012) (eds) 'Special Issue: Cyber War and International Law', *Journal of Conflict & Security Law*, 17(2)

CASSIM, Fawzia (2009) 'Formulating Specialised Legislation to Address the Growing Spectre Of Cybercrime: A Comparative Study', *P.E.R.*, 12(4): 36-79

CHEN, Tom, JARVIS, Lee, and MACDONALD, Stuart (2014) (eds) *Cyberterrorism: Understanding, Assessment, and Response*, Berlin: Springer

CLANCY, Thomas K. (2014) *Cyber Crime and Digital Evidence: Materials and Cases* (second edition), Durham (North Carolina): Carolina Academic Press

COHEN, Aviv (2010) 'Cyberterrorism: Are We Legally Ready?', *Journal of International Business and Law*, 9(1): 1-40

COHEN, Aviv (2012) 'Prosecuting Terrorists at the International Criminal Court: Reevaluating an unused legal tool to combat terrorism, *Michigan State International Law Review*, 20(2): 219-257

COHEN, Frederick B. (2010) 'Fundamentals of Digital Forensic Evidence', in STAVROULAKIS, Peter, and STAMP, Mark (eds) *Handbook of Information and Communication Security*, Berlin: Springer, pp. 789-808

D'ASPREMONT, Jean (2016) 'Cyber Operations and International Law: An Interventionist Legal Thought', *Journal of Conflict and Security Law*, 21(3): 575-593

EastWest Institute (2010) Global Cyber Deterrence: Views from China, the U.S., Russia, India, and Norway, available online at: https://www.files.ethz.ch/isn/115239/2010-04_GlobalCyberDeterrence.pdf

EDWARDS, Lilian, and WAELDE, Charlotte (1998) (eds) *Law and the Internet: Regulating Cyberspace* (first edition), Oxford: Hart Publishing [especially chapter 12, by Paul Benedict CULLEN]

EDWARDS, Lilian, and WAELDE, Charlotte (2009) (eds) *Law and the Internet* (third edition), Oxford: Hart Publishing [especially chapters 17, by Judith RAUHOFER, and 21, by Ian BROWN, Lilian EDWARDS and Christopher T. MARSDEN]

FAHEY, Elaine (2014) 'EU'S Cybercrime and Cyber Security Rule-Making: Mapping the Internal and External Dimensions of EU Security', *European Journal of Risk Regulation*, 5(1): 46-60

FANENBRUCK, Christina, and MEIßNER, Lenya (2015) *Supranational courts as engines for regional integration? A comparative study of the Southern African Development Community Tribunal, the European Union Court of Justice, and the Andean Court of Justice*, available online at: http://nbn-resolving.de/urn:nbn:de:0168-ssoar-453448

FIDLER, David P. (2016) 'Cyberspace, Terrorism and International Law', *Journal of Conflict and Security Law*, 21(3): 475-493

FOGGETTI, Nadina (2015) 'Cyber Terrorism and the reconstruction of customary rule about terrorism of the Special Tribunal for Lebanon in the recent case law', *Ius Et Scientia,* 1(1): 54-78

GERCKE, Marco (2010) 'Challenges in Developing a Legal Response to Terrorist Use of the Internet', *Defence Against Terrorism Review*, 3(2): 37-58

GIACOMELLO, Giampiero (2008) *National Governments and Control of the Internet: A Digital Challenge* (reissued edition), Abingdon-on-Thames: Routledge, chapter 3

GRAHAM, David E. (2010) 'Cyber Threats and the Law of War', *Journal of National Security Law & Policy*, 4: 87-102

GRILLO, Ralph, BALLARD, Roger, FERRARI, Alessandro, HOEKEMA, André J., MAUSSEN, Marcel, and SHAH, Prakash (2009) (eds) *Legal Practice and Cultural Diversity*, Farnham (Surrey): Ashgate

HATHAWAY, Oona A., and CROOTOF, Rebecca (2012) *The Law of Cyber-Attack*, available online at: http://digitalcommons.law.yale.edu/fss_papers/3852

HELFER, Laurence R., and SLAUGHTER, Anne-Marie (2005) 'Why States Create International Tribunals: A Response to Professors Posner and Yoo', *California Law Review*, 93: 1-58

HOSEIN, Gus (2006) 'Policy Laundering, and Other Policy Dynamics', in HALPIN, Edward, TREVORROW, Philippa, WEBB, David, and WRIGHT, Steve (eds) *Cyberwar, Netwar and the Revolution in Military Affairs*, Basingstoke (Hampshire): Palgrave Macmillan, pp. 228-241

HUGHES, Rex (2010) *Towards a Global Regime for Cyber Warfare*, available online at: http://www.ccdcoe.org/publications/virtualbattlefield/07_HUGHES%20Cyber%20Regime.pdf

International Telecommunication Union (2008) *Global Cybersecurity Agenda – Strategic Report*, available online at: https://ccdcoe.org/sites/default/files/documents/ITU-080801-HLEGreport.pdf

JACOB, Frank (2011) 'Cyber-Terrorism', in SPRINGER, Paul J. (ed) *Encyclopedia of Cyber Warfare*, Santa Barbara (California): ABC-CLIO, pp. 67-70

JASTRAM, Kate, and QUINTIN, Anne (2011) *The Internet in Bello: Cyber War Law, Ethics and Policy*, available online at: https://www.law.berkeley.edu/wp-content/uploads/2015/04/cyberwarfare-seminar-summary-complete.pdf

JARVIS, Lee, and MACDONALD, Stuart (2015) *Responding to cyberterrorism: Options and avenues. Georgetown Journal of International Affairs*, available online at: https://ueaeprints.uea.ac.uk/55688/

JUPILLAT, Nicolas (2015) 'Armed Attacks in Cyberspace: The Unseen Threat to Peace and Security that Redefines the Law of State Responsibility', *University of Detroit Mercy Law Review*, 92: 115-129

KANUCK, Sean (2010) 'Sovereign Discourse on Cyber Conflict Under International Law', *Texas Law Review*, 88: 1571-1597

KESIDIS, George (2011) 'Denial-of-Service Detection', in VAN TILBORG, Henk C. A., and JAJODIA, Sushil (eds) *Encyclopedia of Cryptography and Security* (second edition), Berlin: Springer, pp. 323-328

KITTICHAISAREE, Kriangsak (2017) *Public International Law of Cyberspace*, Berlin: Springer

KOHL, Uta (2007) *Jurisdiction and the Internet: A Study of Regulatory Competence over Online Activity*, Cambridge (England): Cambridge University Press [especially chapter 6]

KORSTANJE, Maximiliano E. (2016) *Threat Mitigation and Detection of Cyber Warfare and Terrorism Activities*, Hershey (Pennsylvania): IGI Global

KRAFT, W. (2011) *Ideas on the Establishment of an International Court for Cyber Crime*, available online at: www.wclf.de/cybercrime_court_en.html?file=tl_files/Media/Download/CYBER-COURT-ENGLISH.pdf

LEVMORE, Saul, and NUSSBAUM, Martha Craven (2010) (eds) *The Offensive Internet: Speech, Privacy, and Reputation*, Cambridge (Massachusetts): Harvard University Press [especially chapter 3, by Saul LEVMORE]

LI, Xingan (2007) *International Actions against Cybercrime: Networking Legal Systems in the Networked Crime Scene*, available online at: http://www.webology.org/2007/v4n3/a45.html

LINAKI, Evangelia (2014) 'Cyber Warfare and International Humanitarian Law: A Matter of Applicability', *Journal of International Law of Peace and Armed Conflict (German Red Cross)*, 27(4): 169-175

MACDONALD, Stuart (2015) 'Cyberterrorism and Enemy Criminal Law', in OHLIN, Jens David, GOVERN, Kevin H., and FINKELSTEIN, Claire (eds) *CyberWar: Law and Ethics for Virtual Conflicts*, New York: Oxford University Press, pp. 57-75

MAURO, Massimo (2006) 'Threat Assessment and Protective Measures: Extending the Asia-Europe Meeting IV Conclusions on Fighting International Terrorism and Other Instruments to Cyber Terrorism', in HALPIN, Edward, TREVORROW, Philippa, WEBB, David, and WRIGHT, Steve (eds) *Cyberwar, Netwar and the Revolution in Military Affairs*, Basingstoke (Hampshire): Palgrave Macmillan, pp. 219-227

MELZER, Nils (2011) *Cyberwarfare and International Law*, available online at: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf

MENKEL-MEADOW, Carrie (2011) 'Why and How to Study "Transnational" Law', *UC Irvine Law Review*, 1(1): 97-129

MOORE, Stephen (2013) 'Cyber Attacks and the Beginnings of an International Cyber Treaty', *North Carolina Journal of International Law and Commercial Regulation*, 39(1): 223-257

MUSIANI, Francesca (2009) *The Internet Bill of Rights project: The challenge of reconciliation between natural freedoms and needs for* regulation, Fourth Annual GigaNet Symposium in Sharm-el-Sheikh, available online at: https://hal.archives-ouvertes.fr/hal-00448248/document

OGUN, Mehmet Nesip (2015) *Terrorist Use of Cyberspace and Cyber Terrorism: New Challenges and Response,* NATO Science for Peace and Security Series - D: Information and Communication Security, Amsterdam: IOS Press

OPHARDT, Jonathan A. (2010) 'Cyber Warfare and the Crime of Aggression: The Need for Individual Accountability on Tomorrow's Battlefield', *Duke Law & Technology Review*, 3, available online at: http://scholarship.law.duke.edu/dltr/vol9/iss1/2/

PFÖSTL, Eva (2008) *Sicurezza e libertà fondamentali*, Rome: Editrice Apes, chapters 3 and 5

POLAŃSKI, Paul Przemysław (2007) *Customary Law of the Internet: In the Search for a Supranational Cyberspace Law*, The Hague (Netherlands): TMC [especially chapters 4 and 10]

Police Executive Research Forum (2014) *The Role of Local Law Enforcement Agencies in Preventing and Investigating Cybercrime*, available online at: http://www.policeforum.org/assets/docs/Critical_Issues_Series_2/the%20role%20of%20local%20law%20enforcement%20agencies%20in%20preventing%20and%20investigating%20cybercrime%202014.pdf

PRASAD, Krishna (2012) *Cyberterrorism: Addressing the Challenges for Establishing an International Legal Framework*, available online at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1016&context=act

PROULX, Vincent-Joël (2012) *Transnational Terrorism and State Accountability: A New Theory of Prevention*, London: Bloomsbury Publishing

RADZIWILL, Yaroslav (2015) *Cyber-Attacks and the Exploitable Imperfections of International Law*, Leiden (The Netherlands): BRILL

REICH, Pauline C., WEINSTEIN, Stuart, WILD, Charles, and CABANLONG, Allan S. (2010) 'Cyber Warfare: A Review of Theories, Law, Policies, Actual Incidents - and the Dilemma of Anonymity', *European Journal of Law and Technology*, 1(2), available online at: http://ejlt.org/article/view/40/58

ROSCINI, Marco (2010) 'World Wide Warfare: *Jus ad bellum* and the use of cyber force', *Max Planck Yearbook of United Nations Law*, Leiden (Netherlands): Martinus Nijhoff Publishers, pp. 85-130

SAQF AL-HAIT, Adel Azzam (2014) 'Jurisdiction in Cybercrimes: A Comparative Study', *Journal of Law, Policy and Globalization*, 22: 75-84

SCHABAS, William Anthony, and MCDERMOTT, Yvonne (2013) (eds) *The Ashgate Research Companion to International Criminal Law: Critical Perspectives*, Farnham (England): Ashgate

SCHMITT, Michael N. (2014) '"Below the Threshold" Cyber Operations: The Countermeasures Response Option and International Law', *Virginia Journal Of International Law*, 54(3): 697-732

SCHMITT, Michael N. (2014) 'The Law Of Cyber Warfare: Quo Vadis?', *Stanford Law & Policy Review*, 25: 269-299

SHULL, Aaron (2014) *Global Cybercrime: The Interplay of Politics and Law*, available online at: https://www.cigionline.org/sites/default/files/no8_1.pdf

SMITH, Russell G., CHAK-CHUNG CHEUNG, Ray, YIU-CHUNG LAU, Laurie (eds.) (2015) *Cybercrime Risks and Responses: Eastern and Western Perspectives*, London: Palgrave Macmillan

SOFAER, Abraham David, and GOODMAN, Seymour E. (2001) (eds) *The Transnational Dimension of Cyber Crime and Terrorism*, Stanford (California): Hoover Institution Press [especially chapter 2, by Tonya Lee PUTNAM and David D. ELLIOTT]

STOCKTON, Paul N., and GOLABEK-GOLDMAN, Michele (2014) 'Prosecuting Cyberterrorists: Applying Traditional Jurisdictional Frameworks to a Modern Threat', *Stanford Law & Policy* Review, 25: 211-268

STONEHOUSE, Joshua C. (2016) *A framework for synthesizing the United States Code in support of cyberspace operations*, available online at: https://calhoun.nps.edu/bitstream/handle/10945/48480/16Mar_Stonehouse_Joshua.pdf

TEHRANI, Pardis Moslemzadeh, ABDUL MANAP, Nazura, and TAJI, Hossein (2013) 'Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime', *Computer Law and Security Review*, 29(3): 207-215

The Project on International Courts and Tribunals (2004) *The International Judiciary in Context*, available online at: http://www.pict-pcti.org/publications/synoptic_chart/synop_c4.pdf

TRAPP, Kimberley N. (2012) 'Holding States Responsible for Terrorism before the International Court of Justice', *Journal of International Dispute Settlement*, 3(2): 279-298

TSAGOURIAS, Nikolaos K., and BUCHAN, Russell (2015) (eds) *Research Handbook on International Law and Cyberspace*, Cheltenham (England): Edward Elgar Publishing

U.S. Department of Justice (2007) *Digital Evidence in the Courtroom: A Guide for Law Enforcement and Prosecutors*, available online at: https://www.ncjrs.gov/pdffiles1/nij/211314.pdf

UERPMANN-WITTZACK, Robert (2010) 'Principles of International Internet Law', *German Law Journal*, 11(11): 1245-1263

United Nations Office on Drugs and Crime (2010), *The Globalization of Crime: A Transnational Organized Crime Threat Assessment*, available online at: https://www.unodc.org/documents/data-and-analysis/tocta/TOCTA_Report_2010_low_res.pdf

United Nations Office on Drugs and Crime (2012), *The use of the Internet for terrorist purposes*, available online at: https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

VENTRE, Daniel (2013) (ed) *Cyber Conflict: Competing National Perspectives*, Hoboken (New Jersey): John Wiley & Sons

VOGEL, Joachim (2007) *Towards a Global Convention against Cybercrime*, available online at: http://www.penal.org/sites/default/files/files/Guadalajara-Vogel.pdf

WALL, David S. (2009) (ed) *Crime and Deviance in Cyberspace*, Farnham: Ashgate

YAO-CHUNG CHANG, Lennon (2012) *Cybercrime in the Greater China Region: Regulatory Responses and Crime Prevention Across the Taiwan Strait*, Cheltenham: Edward Elgar

APPENDIX

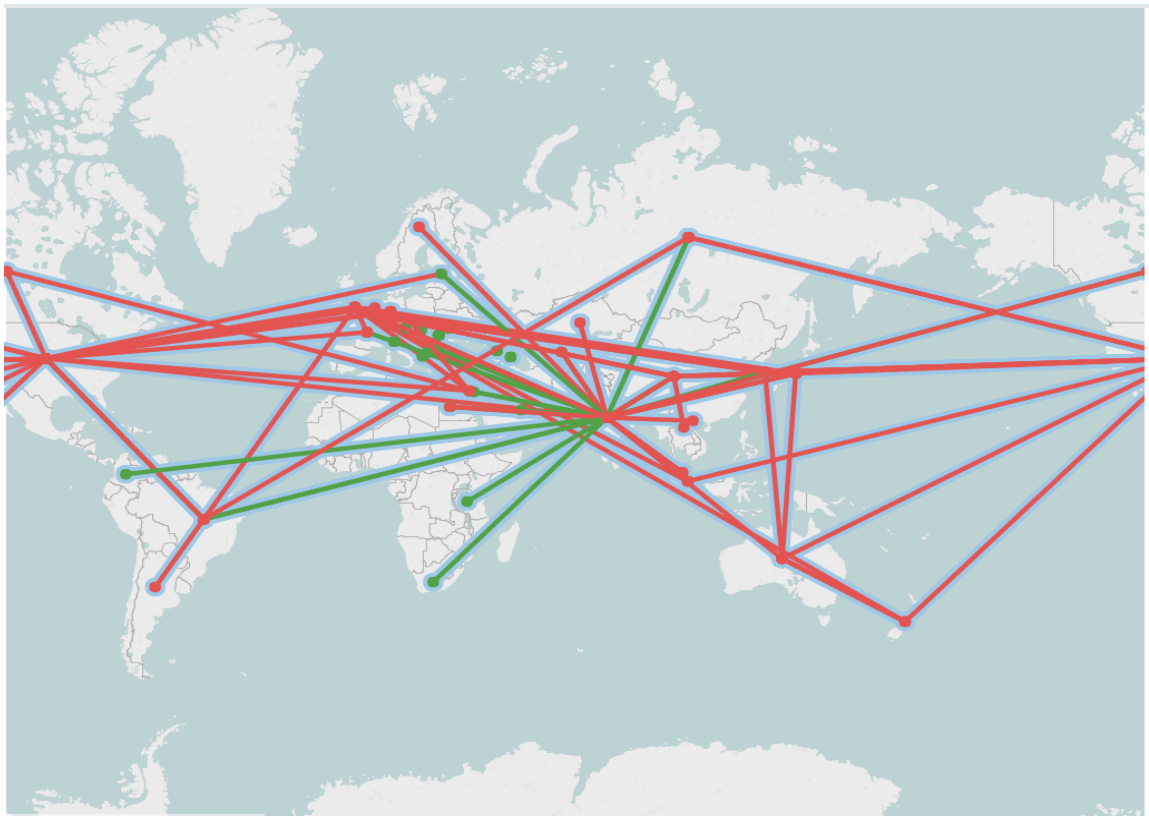

Fig. 1: DiploFoundation (2017) *Bilateral cyber relationships* [including agreements/treaties, dialogues, and statements/communiqués, where red-coloured lines represent cyber & cybersecurity relations, and green represent ICT/information society and e-governance], available online at: https://public.tableau.com/profile/publish/cyberagreements/Dashboard1#!/publish-confirm

Region	Legal	Technical	Organizational	Capacity Building	Cooperation
AFR	0.29	0.18	0.16	0.17	0.25
AMS	0.40	0.30	0.24	0.28	0.26
ARB	0.44	0.33	0.27	0.34	0.29
ASP	0.43	0.38	0.31	0.34	0.39
CIS	0.58	0.42	0.37	0.38	0.40
EUR	0.61	0.60	0.45	0.49	0.46

Fig. 2: *Global Cybersecurity Index 2017 Regional Grid*, International Telecommunications Union, available online at: https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [p. 25]

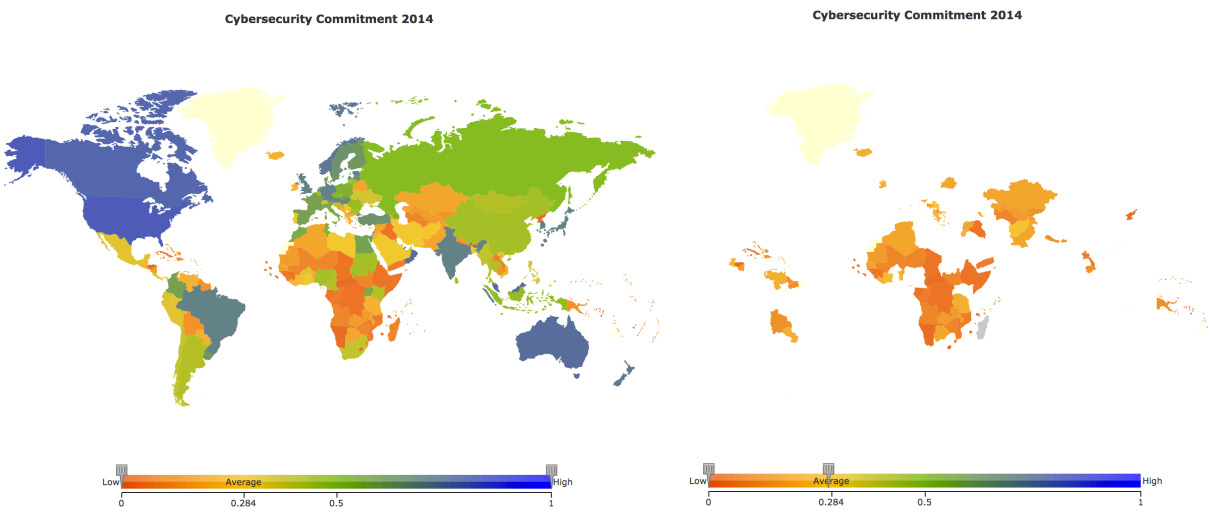

Fig. 3: Comparison: overall Cybersecurity Commitment levels vs Regions with Low Cybersecurity Commitment in 2014, source: http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_heatmap.aspx

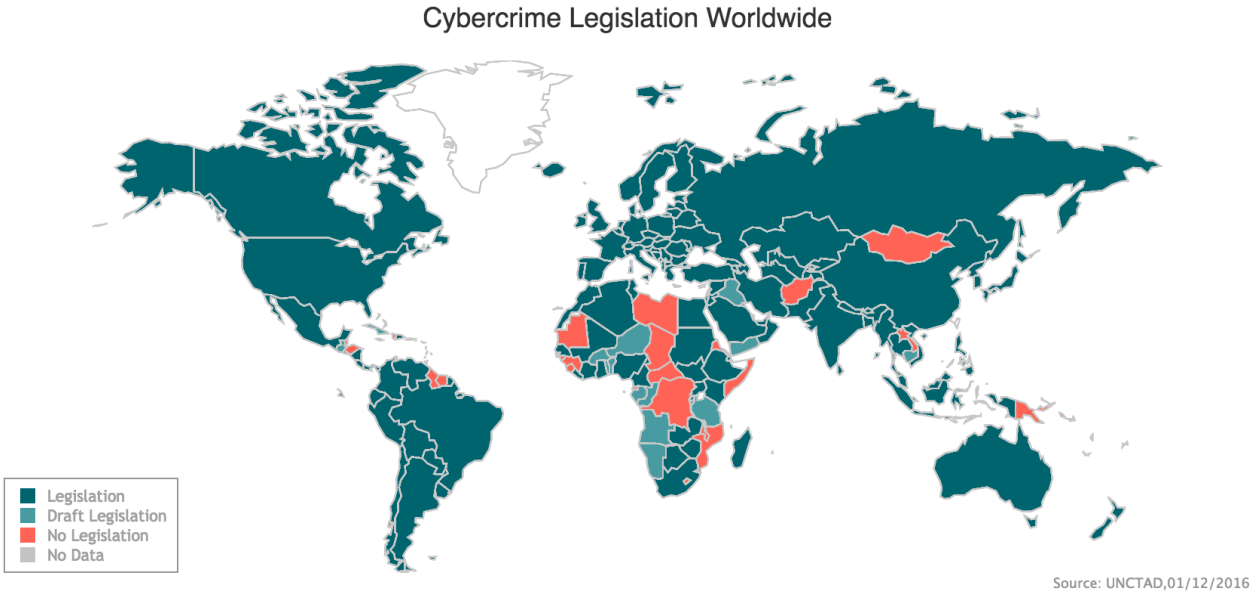

Fig. 4: UNCTAD (2016) *Cybercrime legislation worldwide*, available online at: http://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx

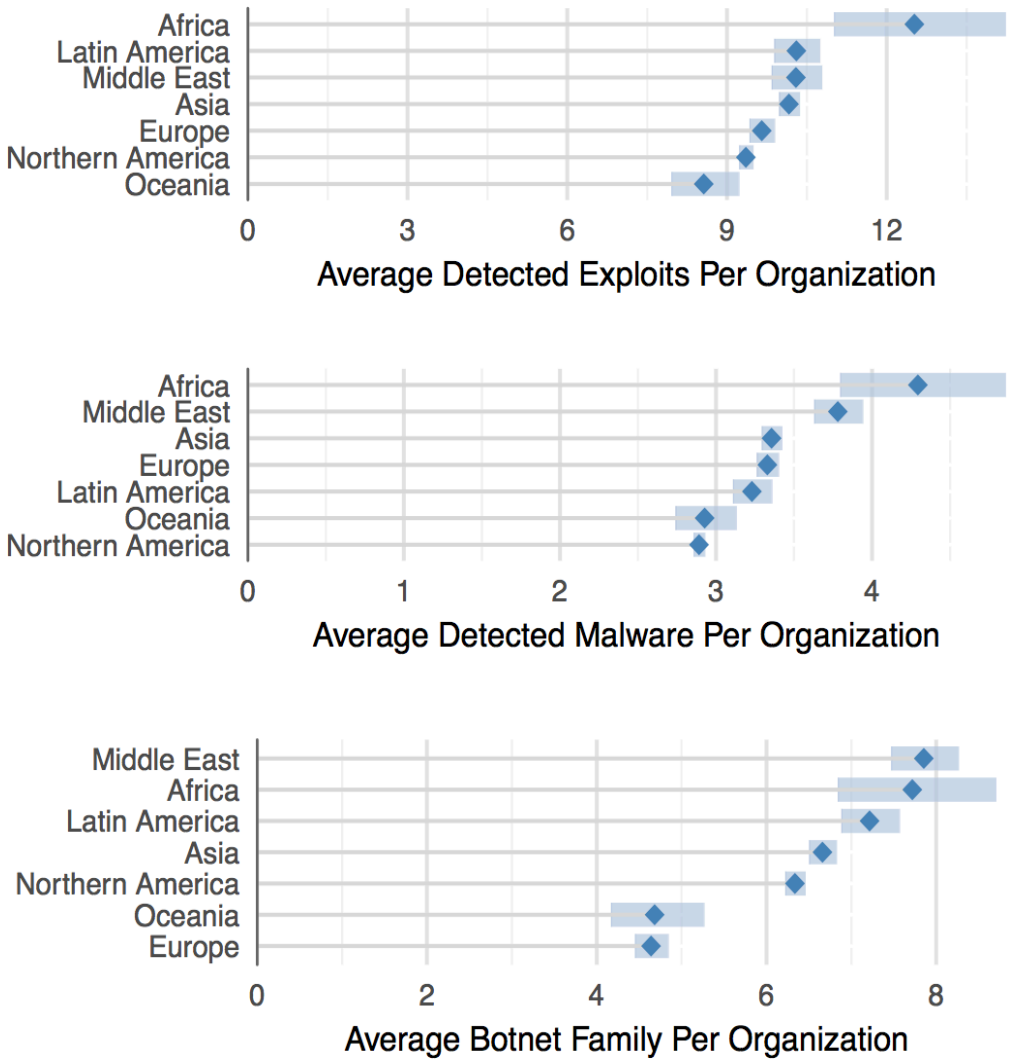

Fig. 5: Fortinet (2016) *Threat Landscape Report Q4 2016*, available online at: https://www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report.pdf [p. 22]