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

INTRODUCTION AND FIRST PART

Olesya DOVGALYUK
BSc Student in Politics and International Relations, SPAIS, FSSL, University of Bristol (UK)
Riccardo VECELLIO SEGATE
MSc Student in European and Global Governance, SPAIS, FSSL, University of Bristol (UK)

London
March 2017

Abstract

The ultimate aim of this article is to analyse the role of the rising and already-existent regional courts in adjudicating terrorism as it appears in the Public International Law against the wider framework of global counter-terrorism struggle, with a special focus on the emerging category of cybercrimes/cyberterrorism, all exceptionally challenging due to the absence of the universally-agreed legal definitions or agreement on the elements constituting either of these crimes. Applying comparative law, we proceed to assess whether and how different legal frameworks and traditions – such as civil law, common law, sharia law and socialist/communist law – affect judicial cooperation between territories and regional institutions. A distinction between the first- and second-generation institutions is also made, with the conclusion that the latter (as organizations focused on trade and economic issues) drive judicial cooperation more effectively due to their more neutral outlook and greater incentives for the member-states pursuing their national interests, to comply with the rules.

OUTLINE CONTENTS

INTRODUCTION

Do we need to rethink how international […] law applies in a world where we're all so dependent on computer systems? [1]

Among intra- and interstate conflicts, the rise of secessionist and nationalist movements, and overarching social disintegration dynamics in general, internationalisation of the judiciary seems an ever-bleak, antithetical against this background perspective. The 'disaggregation of the state and the rise of a plurality of sources of rules […], the gap between formal legality and the law in practice […], and the necessity of a multi-disciplinary approach'[2] are typical characteristics of the international judicial fora nowadays.

This can be clearly traced through the changes in the public attitude to the once respected and trusted institutions. For example, the legacy of International Criminal Tribunals for Rwanda and former Yugoslavia has recently been questioned in relation to the introduced concept of "specific direction"[3] and a related implication that some of the Courts' members are working under US agenda.[4] International Criminal Court is also a subject to numerous criticisms for its: estimated $1b+ budget over a decade; two "cases" (DRC and Mali) with four convicted defendants only; claimed bias with the majority of dossiers on the crimes committed in Africa (although, comparing the number of *referred* and *prosecutor-initiated* investigations it turns out that the accusers themselves make misinformed judgements); resultant from political constraints inability to enforce neglected convictions (e.g. in the case of Omar al-Bashir); and subsequently disputed 'legitimacy as an authentic interpreter of international norms'.[5,6]

Put simply, now, more than ever, is the time when real power of many international judicial bodies based on claimed *universal* jurisdiction is being questioned. This is especially relevant for the cases when the very legal basis for criminal adjudication is murky, ill-defined and open for relativist interpretations, such as those involving matters of terrorism. The latest example (as of March 6, 2017) is the lawsuit brought by Ukraine against Russia[7] to the

---

[1] FERRIS, Elizabeth (2014) 'Why Humanitarians Should Pay Attention to Cybersecurity', *Brookings*, June 2, available online at: https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/

[2] MURPHY, Cian C. (2016) 'The dynamics of transnational counter-terrorism law: towards a methodology, map, and critique' in JACKSON, Vicki, and FABBRINI, Federico (eds.) *Constitutionalism across Borders in the Struggle Against Terrorism*, available online from: https://www.elgaronline.com/view/9781784715380.00014.xml [p. 79]

[3] for the discussion of problems linked to this concept, such as indirect aid to irregular and paramilitary forces, and other secondary agents across different cases, see: http://www.nytimes.com/2013/07/10/opinion/global/a-tribunals-legal-stumble.html, http://www.nytimes.com/2013/05/17/world/middleeast/russia-provides-syria-with-advanced-missiles.html?pagewanted=all

[4] WALLIS, Andrew (2014) 'International justice and Rwanda: Has the UN failed again?', *Al Jazeera*, April 26, available online at: http://www.aljazeera.com/indepth/opinion/2014/04/international-justice-rwanda-u-2014417153532217202.html

[5] DAVENPORT, David (2014) 'International Criminal Court: 12 Years, $1 Billion, 2 Convictions', *Forbes Opinion*, available online at: https://www.forbes.com/sites/daviddavenport/2014/03/12/international-criminal-court-12-years-1-billion-2-convictions-2/#3188bd6f2405

[6] DANNER, Allison Marston (2005) 'Prosecutorial discretion and legitimacy', *Guest Lecture Series of the Office of the Prosecutor,* June 13, The Hague, available online at: https://www.icc-cpi.int/NR/rdonlyres/69ACE89D-D3CA-4D4F-9356-3A3DD1238E65/0/050613_Danner_presentation.pdf

[7] ICJ (2017) 'Ukraine institutes proceedings against the Russian Federation and requests the Court to indicate provisional measures', *(Unofficial) Press Release No. 2017/2*, January 17, available online at: http://www.icj-cij.org/docket/files/166/19310.pdf

International Court of Justice (ICJ) in The Hague; among several accusations brought up against the latter – mostly related to the annexation of Crimea and the conflict in Eastern Ukraine – Russia is blamed for financing terrorism (specifically linked to the Russian BUK missile system, used in the MH17/MAS17 Flight shot-down) in spite of the 1999 International Convention for the Suppression of the Financing of Terrorism.[8] The verdict and the enforcement thereof – considering Russia's veto power in the Security Council and the failure of the UN so far to adopt a single straightforward definition of terrorism[9] – will show how effective ICJ might be in the matters related to international terrorism.

International community is stuck in the situation when national governments are left to use the loopholes to their own advantage.[10] The inability to address it likely comes from the fact that most of the first-generation institutions of world governance have been heavily West-driven, and therefore do not reflect the current multilateral nature of power balance in a multipolar world, undermining regional actors' trust in global governance organizations.[11] These 'doubts about the efficacy of the big multilaterals, and the demand for more justice and equity from the developing countries'[12] signify a pressing demand for alternative practical mechanisms and conceptual solutions for international adjudication.

Cyberspace

Pace of technological development in the aforediscussed context only raises more contradictions and disputes around the attempts to define and prosecute terrorism, which appears more distorted and mutated in cyberspace. Although the latter as such has been present in our life long enough, cyber-attacks and e-terrorism are relatively recent phenomena: for

---

[8] http://www.bbc.co.uk/news/world-europe-39177504, http://www.politico.eu/article/ukraine-takes-terrorism-case-against-russia-to-international-court/. For the full text of the mentioned Convention see: http://www.un.org/law/cod/finterr.htm

[9] one of the most promising arrangements, according to VAN GINKEL (2012), is the Resolution S/RES/1566 (2004), which in Art.3 describes terroristic acts as

> *criminal acts, including against civilians, committed with the intent to cause death or serious bodily injury, or taking of hostages, with the purpose to provoke a state of terror in the general public or in a group of persons or particular persons, intimidate a population or compel a government or an international organization to do or to abstain from doing any act, which constitute offences within the scope of and as defined in the international conventions and protocols relating to terrorism*

(The UN Security Council's resolution, however, did not state explicitly its aim to set this particular description as a definitive interpretation of the term). See further: VAN GINKEL, Bibi (2012) 'Combating Terrorism: Proposals for Improving the International Legal Framework' in CASSESE, Antonio (ed.) *Realism, Utopia and the Future of International Environmental Law*, Oxford: Oxford University Press

[10] A relatively recent, although likely Western-biased, illustration is the criticism of the "generality" of the Ethiopian Anti-Terrorist Proclamation (652/2009), allowing the TPLF (Tigray People's Liberation Front) to terrorise minorities in opposition to the government. For the full text of the Proclamation see: http://www.ilo.org/dyn/natlex/docs/ELECTRONIC/85140/95140/F260526391/ETH85140.pdf; for the defensive comparative analysis of the Proclamation and its Western counterparts see: http://www.aigaforum.com/articles/Ethiopia-anti-terrorism.pdf

[11] ACHARYA, Amitav (2016) 'The Future of Global Governance: Fragmentation May Be Inevitable and Creative', *Global Governance*, 22: 453-460 [pp. 454-455]

[12] ibid. [p. 455]; for a discussion on the waning support for the International Criminal Court (as an indication of the broader dissatisfaction with the Western-dominated institutions in the field of Public International Law) see DOVGALYUK & VECELLIO SEGATE (available online from: http://www.filodiritto.com/articoli/2017/01/from-russia-and-beyond-the-icc-global-standing-while-countries-resignation-is-getting-serious.html)

example, the United States Institute for Peace 2004 Special Report, while pointing at the 'fear of random, violent victimization [that] blends well with the distrust and outright fear of computer technology', stated that by that point in time 'no single instance of real cyberterrorism ha[d] been recorded'.[13] These fears were confirmed only a couple of years later, with a DDoS in the technologically-dependent Estonia (that uses 'internet for everything from parking to banking to voting'[14]) in 2007, followed by implicit accusations of Kremlin's hand behind the attack, the establishment of NATO CCD COE in Estonian capital Tallinn[15] and a general dilemma of clearly defining 'the meaning of "force" in the twenty-first century' to clarify the circumstances justifying a military response.[16]

Presently, thirteen years on, cyberterrorism and other offensive cyber operations are an undeniable everyday reality for both individual actors (private citizens, public figures, state officials) and collective structures (governments, businesses, non-profit organizations, public services and so on), (prospectively) suffering from the absence of proper cyberspace governance. In economic realm, '[n]ews about successful hacks of large companies[17] seem to have become common place'[18]; in politics, the most recent example concerns presidential elections in the US which have raised a wave of controversy in relation to the likely Russian hacking into the Democratic National Committee computer systems.[19] Dependence on the Internet has placed under threat even such actors as supposedly-neutral humanitarian aid agencies, whose online platforms for donations and databases with personal (including biometric) refugee information are arguably less secure and 'easier for a cybercriminal to hack into', turning it into 'a life or death issue if [the data] falls into the wrong hands'.[20] In response

---

[13] WEIMANN, Gabriel (2004) *Special Report 119* – 'Cyberterrorism: How Real Is the Threat?', US Institute for Peace, available online from: http://www.usip.org/publications/cyberterrorism-how-real-the-threat [pp. 2-3]; the Report also provides an accessible comparison between cyberterrorism and other types of virtual offences, such as "hacktivism" and its sub-instruments of "virtual blockade", "swarming", etc.

[14] for further discussion of the digitally-advanced Estonia see: http://www3.weforum.org/docs/WEF_Entrepreneurship_in_Europe.pdf; http://www.wired.co.uk/article/digital-estonia

[15] for CCD COE research and work see: https://ccdcoe.org/sites/default/files/multimedia/pdf/InternationalCyberNorms_full_book.pdf, https://ccdcoe.org/sites/default/files/multimedia/pdf/CyCon_2014.pdf, https://cryptome.org/2014/01/nato-peacetime-cyberspace.pdf, https://www.law.upenn.edu/institutes/cerl/conferences/cyberwar/papers/reading/Geers.pdf; for the discussion of the legal aspects of cyberwarfare in relation to institutions like NATO, see: https://www.internationalespectator.nl/pub/2016/6/_/pdf/IS_2016_6_ducheine.pdf

[16] DINNISS, Heather Harrison (2012) 'Computer network attacks as a use of force in international law', in *Cyber Warfare and the Laws of War,* Cambridge: Cambridge University Press, available online from: https://www.cambridge.org/core/books/cyber-warfare-and-the-laws-of-war/8B7754F0551FA9E7506DA7A85763CAD8

[17] the most wide-scale recent attacks have been, probably, those on Yahoo: http://www.telegraph.co.uk/technology/2016/12/15/yahoo-hack-need-know-biggest-data-breach-history/ and Sony: http://nics.syr.edu/wp-content/uploads/2016/04/Inside-the-Hack-of-the-Century.pdf; http://www.pocket-lint.com/news/131937-sony-pictures-hack-here-s-everything-we-know-about-the-massive-attack-so-far

[18] DAWSON, Gregory, and DESOUZA, Kevin Clyde (2015) 'How state governments are addressing cybersecurity', *Brookings*, March 5, available online at: https://www.brookings.edu/blog/techtank/2015/03/05/how-state-governments-are-addressing-cybersecurity/

[19] MENN, Joseph (2017) 'U.S. inquiries into Russian election hacking include three FBI probes', *Reuters*, February 18, available online at: http://www.reuters.com/article/us-usa-trump-russia-cyber-idUSKBN15X0OE

[20] FERRIS, Elizabeth (2014) 'Why Humanitarians Should Pay Attention to Cybersecurity', *Brookings*, June 2, available online at: https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/

to the 'exposed vulnerabilities in their digital infrastructure'[21], governments are establishing special agencies and institutions to protect their critical online data-storage skeletons – metaphorically speaking, building up immune systems as opposed to the 'motte and palisade to keep our [e-]bailey inviolate', since '[i]t is not a binary question of whether the system is secure or not, but a question of degree, of how vulnerable, how healthy, how well protected [it] is'.[22] On the international level, the UN Security Council resolution 2322 (2016), which calls for judicial cooperation in the matters of international terrorism, deserves special mentioning as pointing 'at the continuing use, in a globalized society, by terrorists and their supporters, of information and communications technologies, in particular the Internet, to facilitate terrorist acts, […] to incite, recruit, fund or plan terrorist acts'.[23]

The problem, if simplified, lies in the fact that 'cyber threats often come from overseas, making it difficult for law enforcement to deter or punish them, [especially because they] rarely rise to the level that would warrant a military response'.[24] Thus proper cross-border cybergovernance is needed, for which common legislature has to be created – or the existent one updated – to address extreme ambiguity around the concepts of sovereignty, territoriality and intent in the reality with no national borders and plentiful opportunities to hide identity. So far in the "international" aspect of cyber realm, 'treaties have largely focused on implementing domestic cybercrime laws and have done relatively little to address cybersecurity standards, leaving such decisions to the private sector'.[25] Because of the consequently blurred war-peace borders in this dimension yet commonly-resultant collateral damage for civilian infrastructures from the initially targeted military systems[26] (due to the possible use of neutral telecommunications infrastructure), it is difficult to identify a 'precise threshold at which cyber operations should amount to an internationally wrongful threat or use of force'[27] to trigger an open warfare as a result.[28] This state of cyber operations being 'inherently transborder'

---

[21] DINNISS, Heather Harrison (2016) 'Computer networks as a use of force in international law' in *Cyber Warfare and the Laws of War*, Cambridge: Cambridge University Press, available online at: http://bit.ly/2kyiOGv [p. 53]. For a comparison of different definitions of "critical infrastructure" and other terms (of particular interest to this article are "cyber attacks" and "cyberterrorism") see *NATO CCD COE Glossary*: https://ccdcoe.org/cyber-definitions.html

[22] BURROWS, Jim (2017) 'Escaping Dark Age Cybersecurity Thinking', *A Medium Corporation*, available online at: https://medium.com/@brons/escaping-dark-age-cybersecurity-thinking-3e7b0c74bda8#.mpjbiuhcv

[23] UN (2016) 'In Fight against Terrorism, Security Council Adopts Resolution 2322 (2016), Aiming to Strengthen International Judicial Cooperation', *UN Meetings Coverage and Press Releases*, December 12, available online at: https://www.un.org/press/en/2016/sc12620.doc.htm. For early warrants on the information security from the UN see the GA resolutions 53/70 (1999) and 55/63 (2001): http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/53/70, https://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf

[24] WALLACE, Ian (2013) 'The Military Role in Cybersecurity Governance', *Brookings*, December 16, available online at: https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/

[25] 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): 1-50*,* available online at: http://chicagounbound.uchicago.edu/cgi/viewcontent.cgi?article=1700&context=cjil

[26] SEGAL, Adam (2016) 'Cyber Attacks Blurring Borders Between War and Peace', *Brink News,* June 28, available online at: http://www.brinknews.com/cyber-attacks-blurring-borders-between-war-and-peace/ [p. 20]

[27] MELZER, Nils (2011) 'Cyberwarfare and International Law', *UNIDIR Resources*, available online at: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [p. 9]

[28] cfr. note 24

frustrates 'any approach to classification based on geographical factors'[29], a problem that the International Group of Experts under Professor SCHMITT came across while deliberating Tallinn Manual, with the resulting majority-consensus on the applicability of the international legal conventions of self-defence, based on the geographical location of cyber activities and civilian cyber infrastructure[30]; the decision, predictably, is not (yet) universally accepted.

Having only touched top-of-the-iceberg controversies emerging in relation to this new type of global threats, what is more or less clear is that 'cyberspace is […] a notional environment and beyond the jurisdiction of any single nation'[31]. This in turn leads us to the analysis of different levels of jurisdiction required with regards to the nature of cyber operations conducted, since labelling cyber activities as certain types of offence, and identifying whether these are

- committed by state agents *(de jure* and *de facto) or* non-state actors
- within the state territory or against foreign targets and
- with an *intent*[32] to violate state's sovereignty, undermine its self-defense capacity or cause, explicitly or implicitly, particular physical harm to its citizens and critical infrastructure alike[33], or spread propaganda and terror[34]

has, as will be argued further, decisive implications for both the necessity and proportionality of actions in response, and for the area of law involved in the ex post facto investigations and prosecutions.[35] Finally, different judiciaries, 'situated on a sliding scale from internationalism to supranationalism'[36], will be examined, with a particular focus on regional courts' effectiveness and cooperation in cybersecurity matters.

---

[29] SCHMITT, Michael N. (2012) 'Classification of Cyber Conflict', *Journal of Conflict & Security Law*, 17(2): 245-260, available online from: https://academic.oup.com/jcsl/article/17/2/245/852811/Classification-of-Cyber-Conflict [p. 246]

[30] NATO (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, available online at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [p. 178]

[31] COLE, Alan, DREW, Philipp, MCLAUGHLIN, Rob, and MANDSAGER, Dennis (2009) *Sanremo Handbook on Rules of Engagement*, International Institute of Humanitarian Law, available online at: http://www.iihl.org/wp-content/uploads/2015/12/ROE-HANDBOOK-ENGLISH.pdf

[32] International Institute of Humanitarian Law in the above-mentioned *Sanremo Handbook in Rules of Engagement* [p. 15] recognises the problems springing from the fact that 'operations in cyberspace are often non-kinetic, making the determination of hostile act and hostile intent difficult', suggesting 'severity, immediacy, directness and effects of the operation' as alternative criteria of the identification process (http://www.iihl.org/wp-content/uploads/2015/12/ROE-HANDBOOK-ENGLISH.pdf)

[33] DENNING, Dorothy Elizabeth (2001) 'Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy', in ARQUILLA, John (ed.) *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica: RAND, available online at: http://www.rand.org/content/dam/rand/pubs/monograph_reports/MR1382/MR1382.ch8.pdf

[34] BUCHAN, Russell (2012) 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', *Journal of Conflict & Security Law*, available online from: https://academic.oup.com/jcsl/article/17/2/212/852771/Cyber-Attacks-Unlawful-Uses-of-Force-or-Prohibited. For a comparative scrutiny of the two interpretations of cyberterrorism, see: AWAN, Imran (2014) 'Debating The Term Cyber-Terrorism: Issues And Problems', *Internet Journal of Criminology,* available online at: http://www.internetjournalofcriminology.com/awan_debating_the_term_cyber-terrorism_ijc_jan_2014.pdf.

[35] JACKSON, Richard (2009) 'The Study of Terrorism after 11 September 2001: Problems, Challenges and Future Developments', *Political Studies Review,* 7(2): 171-184

[36] 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. 14]

PART I: DIMENSIONS OF LEGISLATIVE STRUGGLE

1. Definition of cyberterrorism and applicable Law

Denning: Jus ad Bellum *and Intent*

The expressions "cyber offence" and "cyber terrorism" are sometimes used interchangeably, which – as illustrated below – is largely due to the vagueness in the conceptualisation, especially of the latter, which might come in disguise of the more general former (e.g. malware, DDoS etc.), yet what will differentiate cyberterrorism is the underlying political intent of the attackers as opposed to pure individual interest. As Gordon stated – and this remark would still be relevant today, only stressing the slow progress in the international law-making – '[i]f you ask 10 people what "cyberterrorism" is, you will get at least nine different answers!'.[37]

Definitional gap in the terminology of cyberterrorism, represented by Denning (who defines cyberterrorism as a use of computers to target critical infrastructures and cause 'grave harm such as loss of life or severe economic damage') and Weimann (who perceives cyberterrorism more broadly as a tactic of propaganda-spreading, spread of fear and terrorist recruitment), is essential, and the choice of wording in legislation can say a lot about the underlying intentions of the decision-maker(s). Strong and exclusive preference for Denning's definition would probably show an attempt to project existing *jus ad bellum* to justify aggression in response to the offender, since '[i]n order to constitute an unlawful use of force it is widely accepted that an intervention must produce physical damage'.[38] Implications of such behaviour can be seen in NATO's adoption of *Tallinn Manual*, which, although being "just" a collection of experts' opinions rather than a strictly-binding document, formally reasserted states' right to self-defence in response to cyber (terror) attacks, thereby interpreting art. 2(4) of the UN Charter by stating that 'a cyber operation constitutes a use of force when its scale and *effects* are comparable to non-cyber operations rising to the level of a use of force' [emphasis added].[39] The Manual's revisited version (*Tallinn Manual* 2.0) also added perspectives of International Human Rights, Aviation, and Sea Law to the previously covered *Jus ad Bellum* and International Humanitarian Law. Despite an appreciable breakthrough, however, those experts left a burning question 'of whether a cyber operation of a non-injurious or non-destructive nature […] can reach the armed attack threshold' unanswered, purely because the Manual was a restatement of *lex lata*, not aimed at creating *lex ferenda*.[40] In the consequent absence of a conceptual beacon in this *glossa*-tangle of ambiguous definitions and legal principles (encompassing sociological, securitarian and realpolitik elements), a common among international actors striving for

---

[37] GORDON, Sarah (2003) 'Cyberterrorism?', *Symantec Security Response*, available online at: https://www.symantec.com/avcenter/reference/cyberterrorism.pdf

[38] BUCHAN, Russell (2012) 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', *Journal of Conflict & Security Law*, available online at: https://academic.oup.com/jcsl/article/17/2/212/852771/Cyber-Attacks-Unlawful-Uses-of-Force-or-Prohibited [p. 212]

[39] NATO (2013) *Tallinn Manual on the International Law applicable to Cyber Warfare*, available online at: https://www.peacepalacelibrary.nl/ebooks/files/356296245.pdf [p. 45].

[40] US Naval College (2012) *CyCon 2012 | Michael Schmitt: Tallinn Manual Part I*, available online at: https://www.youtube.com/watch?v=wY3uEo-Itso [3:14-3:20]

Denning's 'effects-based approach [which has already] gained considerable traction in international legal literature, particularly in the context of cyber war', appears an understandable drive for clarity.[41] Thereby, equating certain cyber operations to 'an "armed attack" permits the attacked state to exercise its inherent right to self-defence through means otherwise prohibited by the Charter including, most notably, the resort to force'[42] (this, however, raises an issue of calculating proportionality, one of the key 'elements for determining whether resort to war is justified'[43]). A number of official claims and statements made by governments along these lines portray, in one way or another, critical infrastructure and physical wellbeing of citizens as core criteria to justify an attack in response. The Bush administration has formally stated in the context of the war in Iraq, for instance, that it is the policy of the US to respond to cyberattacks by any means appropriate, including military action. This is not surprising, considering how the US has always been more interested in distancing itself from any norm rather than showing a constructive approach in building new (precise, and preferably binding) international rules. It perceives itself as "the ruler", by definition "beyond the rules", demonstrating not to understand the difference between "security governance" and "legal governance". Although actions in response to the mentioned Russian cyber-intervention in the elections have not been agreed upon yet[44] – as of the moment, the FBI has confirmed investigating Trump's associates for ties to Russian hackers[45] – the fact that both states claim the right of first nuclear attack – notwithstanding the unlikelihood of either opting out for such a scenario – should always be kept at back of one's mind.

The very basis of the phenomenon around which the following discussion revolves therefore looks quite shaky. We do not claim to propose a final verdict on the cyber-dimension reference points: firstly, because it would simply reduce the just-brushed-upon complexity of the legal and non-legal overlapping factors; secondly, because it is not our goal in the first place. We thus allow for a broader combination of the two explanations[46], but our stance somewhat enhances the above-discussed in that it is Denning's definitional elements are indispensable and are to be prioritised. In other words, notions of fear and propaganda ("terror" crucially being an emotional state preceding physical harm) can be misguiding for the case 'where the doer's demands in connection with certain acts are unclear', since terrifying 'the population is a

---

41 BUCHAN, Russell (2012) 'Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?', *Journal of Conflict & Security Law*, available online from: https://academic.oup.com/jcsl/article/17/2/212/852771/Cyber-Attacks-Unlawful-Uses-of-Force-or-Prohibited [p. 217]

42 MELZER, Nils (2011) 'Cyberwarfare and International Law', *UNIDIR Resources*, available online at: http://unidir.org/files/publications/pdfs/cyberwarfare-and-international-law-382.pdf [p. 7]

43 KRETZMER, David (2013) 'The Inherent Right to Self-Defence and Proportionality in *Jus Ad Bellum*', *The European Journal of International Law,* 24(1): 235-282, available online at: http://www.ejil.org/pdfs/24/1/2380.pdf [p. 237]

44 DYER, Geoff (2016) 'US weighs up options in response to Russian hacking', *Financial Times*, October 12, available online at: https://www.ft.com/content/1de86910-9099-11e6-a72e-b428cb934b78

45 ALLEN, Nick, and ALEXANDER, Harriet (2017) 'James Comey confirms the FBI is investigating Donald Trump's associates for ties to Russia', *The Telegraph*, March 20, available online at: http://www.telegraph.co.uk/news/2017/03/20/fbi-confirms-investigation-links-donald-trump-russian-hackers/

46 also often expressed in more general public-oriented sources for the sake of inclusiveness and avoidance of confusion; see, for instance: http://www.informationsecuritybuzz.com/articles/real-threat-cyberterrorism/

[transitional] means to reach some [other ultimate] political objective' and, taken on its own, can result in the principal element of the true *mens rea* (intent) being overlooked by the judiciary.[47]

2. Agency and Territoriality

Intent and Territoriality

As appears obvious at the first sight, '[a]ppreciation of the different motivations behind cyberattacks is essential when seeking ways to address them'.[48] Resultantly, we may wonder if it is mainly a question of international politics or international law. 'Phishing, spam, fabrication of identity, crime in virtual worlds, terrorist use of Internet, and massive and coordinated cyber attacks against information infrastructures'[49] – all these vary in their respective targets and thereby in the scale and severeness of the aftermath effects. Yet in certain cases we are still facing the dilemma of criterion to use for the adjudication process: does the intent really matter if, for instance, 'something goes wrong with a cyberattack intended for a military target and civilians end up as the victims'[50]? Should such unforeseen spillover of the purely criminal act against the (domestic or foreign) government into the area of Human Rights Law be dealt with simultaneously to produce a joint and comprehensive effects-based judgement by a single judiciary, or different institutions with different mandates will have to parcel out "components" of the crime based on their area of competence?

Furthermore, while drawing imaginary borders around the geographical areas affected by cybercrimes and attacks is a problem complicated enough in itself, it is exaggerated by that of statehood, just as in the International Humanitarian Law and International Criminal Law. In this context it is unclear on what basis, for instance, should attacks executed from ungoverned territories be judged. As we discussed elsewhere in relation to the ICC mandate[51], the so-called Islamic State poses a controversial issue to the international judiciary because of its not being a state, exacerbated by non-membership of either Iraq or Syria in the ICC and highly unlikely UNSC referral of the situation due to P5 veto powers. While ISIL's 'online strategy apparently focused more on publicity than damage so far'[52] (and even in this sense it still falls under at least one definition of cyberterrorism, focused on propaganda and fear-spreading) and the

---

47 KASSA, Wondwossen Demissie (2014) 'The Scope of Definition of a Terrorist Act under Ethiopian Law: Appraisal of its Compatibility with Regional and International Counterterrorism Instruments', *Mizan Law Review*, 8(2): 371-405, available online at: https://www.ajol.info/index.php/mlr/article/view/117545 [p. 388]

48 WALLACE, Ian (2013) 'The Military Role in Cybersecurity Governance', *Brookings*, December 16, available online at: https://www.brookings.edu/opinions/the-military-role-in-national-cybersecurity-governance/

49 GHERNAOUTI-HÉLIEA, Solange, and SCHJOLBERG, Stein (2009) 'Global Protocol on Cybersecurity and Cybercrime: an initiative for peace and security in cyberspace', *Cybercrimedata,* available online at: http://www.cybercrimelaw.net/documents/A_Global_Protocol_on_Cybersecurity_and_Cybercrime.pdf [p. 2]

50 FERRIS, Elizabeth (2014) 'Why Humanitarians Should Pay Attention to Cybersecurity', *Brookings*, available online at: https://www.brookings.edu/blog/up-front/2014/06/02/why-humanitarians-should-pay-attention-to-cybersecurity/

51 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: http://www.filodiritto.com/articoli/2017/01/from-russia-and-beyond-the-icc-global-standing-while-countries-resignation-is-getting-serious.html [pp. 13-16]

52 GRAHAM-HARRISON, Emma (2015) 'Could Isis's "cyber caliphate" unleash a deadly attack on key targets?', *The Guardian*, April 12, available online at: https://www.theguardian.com/world/2015/apr/12/isis-cyber-caliphate-hacking-technology-arms-race

skills and crimeware[53] possessed by the group are not yet sufficient enough to pose serious threat to the complex state cybersecurity systems[54], the potential[55] of the United Cyber Caliphate (UCC) growing more professional pushes for the need to resolve the obstructions to the justice enforcement now.

Another point regarding territoriality concerns controversial self-determination statuses of some regions. Embodying this sketch into reality: are we, for example, to "trust" Chinese government to address the cases of 'Tibet and Taiwan [which] have also repeatedly come under attack from alleged Chinese hackers, [even though the latter are] suspected to have the backing of the Chinese government'[56], or presence of an external independent mediator is needed to secure the least bias in the verdict?

All the questions raised so far will be addressed within the framework of analysing specific international and regional institutions further below, and the role of territoriality in the prosecution of cyberterrorism committed by individuals will be considered with regards to the applicability of the ICC mandate to cybercrimes as crimes of aggression/crimes against humanity in the peacetime and war crimes (with the *Jus ad Bellum* and *Jus in Bello* applicable) during the simultaneously ongoing physical conflict. In both cases another factor will have implications for the type of law and level of jurisdiction applicable: the factor in question is state agency behind the cyber offences.

State agents or non-state actors? The issue of Human Rights

As problematised in the introduction, the messy process of identifying the "shadow" of state agency in cyberattacks – at least as it appears from practice – is often fruitless, with the relation between non-state actors and the institution of state responsibility[57] up in the air. A good illustration of this controversy is Russian youth movement "Nashi", who claimed responsibility for the Denial of Service in Estonia, characterising it as a cyber-defence operation; while it seems (at least) highly improbable that a formally independent youth organisation could have had the appropriate level of expertise and been equipped to conduct such a sophisticated offence, it is difficult to deny that 'ingenuity of the [likely but unconfirmed] use [by the Russian government] of "Nashi" as cyberwarfare arm is the group's nominally independent status'.[58]

---

[53] GORDON, Sarah, and FORD, Richard (2006) 'On the definition and classification of cybercrime', *Journal in Computer Virology and Hacking Techniques*, 2: 13-20, available online from: https://link.springer.com/article/10.1007/s11416-006-0015-z [p. 18]

[54] LOHRMANN, Dan (2015) 'Cyber Terrorism: How Dangerous is the ISIS Cyber Caliphate Threat?, *Government Technology*, May 18, available online at: http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html

[55] GALLAGHER, Sean (2016) 'As US drops "cyber bombs", ISIS retools its own cyber army', *Ars Technica UK*, April 28, available online at: https://arstechnica.co.uk/information-technology/2016/04/isis-cyber-army-united-cyber-caliphate-details/

[56] DINNISS, Heather Harrison (2012) 'Computer network attacks as a use of force in international law' in *Cyber Warfare and the Laws of War,* Cambridge: Cambridge University Press, available online from: https://www.cambridge.org/core/books/cyber-warfare-and-the-laws-of-war/8B7754F0551FA9E7506DA7A85763CAD8 [p. 55]

[57] TSAGOURIAS, Nicholas (2016) 'Non-State Actors, Ungoverned Spaces and International Responsibility for Cyber Acts', *Journal of Conflict & Security Law*, 21(3): 455-474

[58] SHACHTMAN, Noah (2009) 'Kremlin Kids: We Launched the Estonian Cyber War', *Wired Security*, November 3, available online at: https://www.wired.com/2009/03/pro-kremlin-gro/

Attempts by the states to gather information on such individuals and private groups for preventive and self-defense purposes, nevertheless, often lead to additional legal problems if made public because of the disproportionate reliance on intelligence agencies which are 'not designed in most legal systems to produce information for use against individuals'.[59] The relative nature of the protective legislature of foreign citizens for foreign agencies means that 'agency from country B will not be so restricted from spying on the nationals of country A' than the country A itself. This legal framework not only leads to violations of many innocent individuals' rights – both in terms of the data-gathering acts themselves (e.g. blacklisting, preventive detention, and "driftnet" surveillance) and the measures used in the process (blackmailing and so forth), – but also in the lack of evidence to use in the global anti-terror campaign as the secretly sourced information usually remains confidential in the court procedures on the matters related to terrorism.[60] The intelligence agencies thus represent another, dangerous dark side of the public-private relationship in the questions related to (cyber)terrorism.

In the end – and in theory – prosecution of individuals has to have clear guidelines: if the crime committed is a national-scale one (e.g. has consequences within the territory of the state where it was perpetrated, and/or the attackers are its citizens), it falls under national mandate. '[I]f they commit conduct that amounts to an international crime' – and a *grave* one – international criminal tribunals, such as ICC, are to get involved.[61] If, however, cyber offences leading to the risks for public safety and wellbeing in particular are planned, financed or executed by state agents, this would require application of Human Rights Law, since '[u]nder the regional systems, only States may be held accountable for human rights violations'.[62] In reality, however, it is – as in the majority of situations when an abstract model is to be applied to the real-world scenarios – complexified by a number of additional factors, among which personal/national interests stand out as one of the most relevant. The common result is well-known: impunity of the few and the suffering of the many.

It is not surprising then that the kind of conflicts we have experienced so far could have been the core reason why humanity has perceived the need to codify and conceptualise the existence of "human rights" enforced by a natural self-evident condition rather than a specific legislative act. As SEN points out, despite the fact that any specific right roots its legitimacy in a previous specific law issued by the "legitimate ruler", it is also true that the so-called "law of nature", as well as generally-perceived "moral rights", 'can serve, and ha[ve] often served in practice, as the basis of new legislation'.[63] What is thus worrying is the event that the new kind of conflicts, such as the cyber ones which are pursued through less tangible means, will be of little impulse in creating new legislation starting from moral rights, since the violation of the latter will inevitably be hidden, covered, less disclosed, less mirrored in the common daily experience of the broad "public opinion". From this perspective, a global legal standing against

---

[59] SCHEPPELE, Kim Lane (2016) 'The deep dilemma of evidence in the global anti-terror campaign', in JACKSON, Vicki C., and FABBRINI, Federico (eds.) *Constitutionalism across Borders in the Struggle Against Terrorism*, available online from: https://www.elgaronline.com/view/9781784715380.00014.xml [p. 146]

[60] Ibid. [pp. 147-151]

[61] limitations of territorial jurisdiction in the Rome Statute, which empowers the ICC to exercise its mandate only when crimes are committed on the territory/against the nationals of its Member States, and the SC referral mechanism for other cases are discussed further down in the Part II of this article

[62] International Justice Resource Center (2014) *Regional Systems*, available online at: http://www.ijrcenter.org/regional/

[63] SEN, Amartya (2010) *The Idea of Justice* (reprinted version), London: Penguin Books [p. 363]

the cyber warfare will be appreciably more difficult to observe in terms of "spillover effect" from the violation of essential, "natural", fundamental rights; consequently, that posture - or put differently, people's reaction - will be confined within the borders of certain communities (more or less geographically extended they are). As a result, we believe that only a "regionalised" legal approach to this matter will potentially reach a consensus. Indeed, a noticeable number of 'actual laws have been enacted by individual states, or by association of states, which gave legal force to certain rights seen as basic human rights'[64]; an occurrence validated by the understanding of major violations such as torture or degrading treatments, and arguably to be expected even more acutely with regards to more "elusive" misdemeanours. Not to mention the fact that cyber warfare or more widely cyber-crimes, when pursued in the sake of a pretended ideal and addressed as terrorism, are imbued with values and ideologies which are inherently linkable to a regional interpretation of what "human rights" truly are.

All this could just appear as a mere philosophical or abstract point, while it is conversely as concrete as the impact of cyber-related crimes on people's interests and safety nowadays. Our future as human beings will also depend upon the extent to which we will be enabled to advocate in order to keep alive the aforementioned "spillover effect" from *moral* rights to *strictly-legal* rights. This is a fight for civilisation and international law's progress, fought in spite of the fact that the online violations will not immediately seem as brutal or unacceptable as a slaughtered, "offline" flesh-and-blood body.

* * * * * * * *

[64] Ibid. [p. 364]