Fragmenting Cybersecurity Norms Through the Language(s) of Subalternity

Vecellio Segate, Riccardo

Published in:
Columbia Journal of Asian Law

DOI:
10.7916/cjal.v32i2.3371

Publication date:
2019

COLUMBIA JOURNAL OF ASIAN LAW
VOLUME 32 SPRING 2019 NUMBER 2

ARTICLES

FRAGMENTING CYBERSECURITY NORMS THROUGH THE LANGUAGE(S) OF SUBALTERNITY: INDIA IN "THE EAST" AND THE GLOBAL COMMUNITY

Riccardo Vecellio Segate[†]

The global cybersecurity discourse has never proved more fragmented than in the aftermath of the failure of the last United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security. This discourse stands trapped in long-lasting and seemingly crystallized normative stances between "the West" and "the East," yet it also calls upon the international community to regulate a wide spectrum of phenomena, ranging from thefts of digitally-stored trade secrets to large-scale pervasive attacks, which may soon reach the threshold of armed attacks. If one situates the major cybersecurity players on a sliding scale between freedom and control over cyber content and infrastructure, the mainstream stance would place the United States, the European Union, the United Kingdom, Brazil, India, China, and Russia in that order. Nonetheless, this scale is in practice more complex, in part due to the influence of

[†] "Talent Program" Ph.D. Researcher in International Law, Faculty of Law, University of Macau (China); Incoming Visiting Fellow, Centre for Law and Technology, Faculty of Law, The University of Hong Kong (China); LL.M. in Public International Law, Utrecht University (The Netherlands); Postgraduate Diploma in European and Global Governance, University of Bristol (UK); Executive Editor of the *Utrecht Journal of International and European Law* (2017–2019). I would like to express my most sincere gratitude to the Editorial Board of this Journal for the impeccable professionalism and praiseworthy patience demonstrated during the editing process. I also extend my deepest thanks to Renmin Law School and the Asian Society of International Law for having hosted the presentation of an earlier version of this paper during the AsianSIL Regional Conference held in Beijing in October 2018. Finally, I am indebted with Ms. Olesya Dovgalyuk (Peking University) for sharing relevant insights on the functioning of the Shanghai Cooperation Organisation. I have neither competing interests to declare, nor funds to acknowledge. Webpages have been last accessed on May 3, 2019; no responsibility can be attributed for later relocation or alteration of online contents. All other possible errors and inaccuracies, as usual, remain my own. Comments can be addressed to r.vecelliosegate@connect.um.edu.mo

the Shanghai Cooperation Organisation, a regional security forum which has witnessed major rebalancing after the membership expansion in June 2017.

This paper scrutinizes India's contribution towards a possible fragmentation of the "Eastern" cybersecurity discourse based on hard laws and state assertiveness, and the consequent disruption of the constructivist East-West binary dialectic about cyberwarfare, cyberterrorism, cyber espionage, and online data protection. By simultaneously negotiating its sub-alterity *and rejecting its* subalternity*, India holds the potential to reshape an otherwise almost-coherent "cyber East."*

I. INTRODUCTION

> To translate . . . means to exchange . . . ; that is to say, to exchange what one has for what one does not have. . . . Neither the translators from the west nor the translators from the east could reach perfection by themselves.[1]

[1] Tang Jingzhao Dajianfusi Yi Jing Zhuan (唐京兆大薦福寺義淨傳) [THE BIOGRAPHY OF YI JING OF THE GREAT JIANFU TEMPLE], *in* 1 AN ANTHOLOGY OF CHINESE DISCOURSE ON TRANSLATION 174, 174 (Martha P.Y. Cheung ed., 2006).

A considerable amount of international law and politics scholarship has been dedicated to cyber-policing over the last fifteen years. This trend parallels the growth, across all territories and social classes, of computer—and especially Internet—technologies in impact, rapidity, and distribution. When a new possible "object" of regulation comes into play on the international plane, the "subjects" of such a possible regulation—primarily but not inevitably states—strive to identify and achieve the correct balance between reliance on already-codified policies and enactment of new object-tailored policies. This is a lengthy process which at times frustrates its promoters, especially because the slow pace is accompanied by a conversely swift crystallization of negotiating stances, which makes it difficult for the dialogue to move forward *en temps utile*.[2] To simplify matters, we can group the regulation of cyber issues in the domain of public international law into at least four categories: Cyberwarfare, cyberterrorism, cyber espionage, and data protection. The last category shares considerable terrain with the private sphere of international law, or "conflict of laws." Said category also intersects with cybercrime more broadly and with intellectual property rights, trade, and commerce. This article focuses on public aspects of cyber-regulations at the international level, and, more specifically, on the *discourses* that have stagnated among different regions of the globe.

At least until recently, one major discourse has shaped the "cyber-norms debate": The one that distinguishes between an "East" and a "West" which are impossible to scientifically define while conceptually quite clear in the mind of many legal and international relations scholars. This cyber-discourse, revolving around endless segmented issues but traversed by a small number of key principles, has witnessed a stalemate originating in the apparent impossibility not only to overcome but even to *understand* the depth and nature of the watershed between "Eastern" and "Western" conceptualizations of those affairs. When the hope for a revival of this debate was fading, new players came into existence, carving out spaces for public international lawyers and diplomats to jump out of established dichotomies and pursue promising new pathways.

Arguably, the most momentous new entrance occurred during the enlargement of the Shanghai Cooperation Organisation (SCO) on June 9, 2017. While the admission of Pakistan did not significantly disrupt the previous "equilibrium," the admission of India has changed the status quo to a truly remarkable degree. Whereas Russia and China held the decision-making scepter before

[2] ROXANA RADU, NEGOTIATING INTERNET GOVERNANCE 157–190 (2019).

India's entry,[3] New Delhi now stands positioned to reorient SCO's strategic choices,[4] which accounts for roughly forty percent of the human population and one quarter of the world's GDP.[5] Some scholars and analysts find this disorienting, as the previous East-West dialectics have relativized, that is, complexified in scope and in variables.[6] China and Russia share common positions on many, albeit not all, global governance issues; as far as this article is concerned, China and Russia possess interchangeable views on cyber matters.[7] India, however, brings to the table completely alien legacies originating from its colonial past, its democratic status, and the peculiarity of its geographical and spiritual features. The field of cyberterrorism was previously characterized by straightforward stances: Fear of internal extremism in "the East," exemplified by SCO members Russia and China,[8] and apprehension of external terrorist threats in "the West," exemplified by the North Atlantic Treaty Organization (NATO) and especially its most prominent member, the United States.[9] In the cyberwarfare field, the divide was no longer about exogenous or endogenous sources of alarm, but

---

[3] Karl Salum, *Russian-Chinese Relations and Their Leadership Potential in the Shanghai Cooperation Organisation*, 17 KVÜÕA TOIMETISED 213, 214 (2013).
[4] *See*, *e.g.*, Meena Singh Roy, *India's Options in the Shanghai Cooperation Organisation*, 36 STRATEGIC ANALYSIS 645, 648 (2012).
[5] Prithvi Ram Mudiam, *The Shanghai Cooperation Organisation and the Gulf: Will India Prefer a Further Westward Expansion of the SCO or its Consolidation?*, 12 ASIAN J. OF MIDDLE EASTERN AND ISLAMIC STUD. 457, 457 (2018); Rick Rowden, *The Rise and Rise of the Shanghai Cooperation Organisation*, SHEFFIELD POLITICAL ECONOMY RESEARCH INSTITUTE GLOBAL POLITICAL ECONOMY BRIEF, Apr. 24, 2018, at 2.
[6] OLIVER STUENKEL, POST-WESTERN WORLD: HOW EMERGING POWERS ARE REMAKING GLOBAL ORDER 6–7 (2016); MARTIN JACQUES, WHEN CHINA RULES THE WORLD: THE RISE OF THE MIDDLE KINGDOM AND THE END OF THE WESTERN WORLD 412 (2009).
[7] Minor differences do exist between Russia's and China's cybersecurity policies; however, as the aim of this article is to frame India's legal and political position between the "Western" and the "Eastern" blocks, a thorough scrutiny of such differences fall well beyond the reach of the present analysis. For more detailed comparison of cyberspace governance in Russia and China, see among many others, Marc Lanteigne, *Russia, China and the Shanghai Cooperation Organisation: Diverging Security Interests and the "Crimea Effect"*, *in* RUSSIA'S TURN TO THE EAST: GLOBAL REORDERING 119–138 (Helge Blakkisrud & Elana Wilson Rowe eds., 2018).
[8] *See generally*, Stephen Aris, *The Shanghai Cooperation Organisation: "Tackling the Three Evils". A Regional Response to Non-traditional Security Challenges or an Anti-Western Bloc?*, 61 EUROPE-ASIA STUD. 457, 457–482 (2009).
[9] *See generally*, Hatice Beril Dedeoğlu, *Bermuda triangle: comparing official definitions of terrorist activity*, 15 TERRORISM AND POLITICAL VIOLENCE 81, 81–110 (2003).

instead focused on the uneven technological preparedness for information warfare between an advanced America and a catching-up Asia. The legal approaches to these fields of activity mirrored these stances so closely that to a certain point scholarship also started to look redundant. However, the revived influence of informal groups such as the BRICS and the admission of India into the SCO have radically transformed a binary discourse into an exceedingly fragmented one, fraught with potentials yet to be exposed. Scholarly displacement is understandable, as public international law has thus come under pressure for stretching its tools in unprecedented and unpredictable ways.

Against the background of such intricacies, and with no claim of an ability to recompose these fractures, the present analysis of state-driven mechanisms will attempt to contribute towards the sophistication of this debate, a process which entails an examination of how the "language of the law" works along the political lines outlined above. Hopefully, this endeavor will offer some tentatively workable frameworks to analyze two interrelated issues: First, to what extent are SCO policies shaping the global agenda on cybersecurity norms? Second, what is the Indian contribution towards the SCO stances on cybersecurity, and how can the poststructuralist focus on negotiating language afford original insights on India's fragmentation of East-West dialectics?

Part II introduces a number of essential elements for analyzing the tensions between Western and Eastern understandings of cyberspace. It starts with the increasingly assertive attitudes of the Chinese government and discloses the meanings attached to "cyber-sovereignty" in Eastern and Western discourses. Then, it sheds light upon India as a strategic "swing state" placed to disrupt the NATO-SCO confrontation while fragmenting the SCO block itself. Part III provides an essential account of the academic debate over informal policymaking strategies and cooperation networks established by states, both among themselves and with international organizations, with the aim of paving the way towards an analysis of the stances enucleated by the SCO regarding the peacetime and wartime governance of cyberspace. Parts IV and V present an in-depth assessment of the aforementioned stances within the SCO, prior to and after the admission of India, respectively. Since it is premature and analytically impossible to scientifically quantify the exact contributions of India to the SCO regarding these matters, this article will analyze the potentialities springing from India as a cyber-actor through analogy. Specifically, this article will merge the initial hints coming from the SCO with Indian patterns of decision-making as a

party to—or partner of—other regional organizations such as the Association of Southeast Asian Nations (ASEAN), the South Asian Association for Regional Cooperation (SAARC), and the British Commonwealth. Part VI situates India and the SCO in the wider picture of international struggles between security and freedom in cyber matters, where key players such as the European Union or the United States advocate—or seem to do so—for confidence-building measures to be adopted on a need-by-need basis, supported by structured and semi-structured organizations like Organization for Security and Co-operation in Europe (OSCE) and the G20. Part VII is dedicated to the study of language as a too-often overlooked bargaining tool and conceptual mindset capable of reversing dominances and overturning perspectives throughout any of the above levels of analysis: The SCO itself, India within the SCO, India vis-à-vis other organizations, India and the SCO versus "the West," and the synthesis of these frameworks before what we define as the "international community." Translations matter, and more importantly, English imperialism still performs its deceitful subjugating function, worsened by a functional appropriation from the East which voids most legal expression of any significance, thereby hindering any advancement in the true comprehension of the particularities of any law under contention.

II. A SUSPICIOUS ENGAGEMENT

> [O]ur common desire and commitment [is] to build a people-centred, inclusive and development-oriented Information Society, . . . premised on the purposes and principles of the Charter of the United Nations and respecting fully and upholding the Universal Declaration of Human Rights.[10]

The multi-stakeholder essence and steadily increasing weaponization of the Internet, coupled with the diversified interdependency among states on information security governance (more broadly, Information and Communications Technologies (ICT) security governance, as preferred in the East; or slightly more

[10] World Summit on the Info. Soc'y (WSIS), *Declaration of Principles*, at 1, WSIS Doc. WSIS-03/GENEVA/DOC/4-E (Dec. 12, 2003).

narrowly, cybersecurity governance, as favored by Western powers),[11] undoubtedly embody an unsolved, if not unsolvable, puzzle for policymakers worldwide, both when it comes to shaping national legislation and when the issue lies with the agreement on basic rules—or "redlines"—among countries.[12] Conservative regimes like the Chinese one abandoned the idea of local communication identities "being watered down in a cultural soup of globalization and Americanization,"[13] to embrace a security-underpinned vision of the cyber-world as a competing arena for divergent societal discourses. In other words, China rerouted its approach from *ideological rejection* to *strategic confrontational engagement*,[14] bringing a period of "ideological irrationality that rejected Western technology and modernization in pursuit of utopian socialism"[15] to its end. As a newly-appointed top Chinese cyberspace official, Mr. Zhuang Rongwen says, "[w]hoever masters the Internet holds the initiative of the era, and whoever does not take the Internet seriously will be cast aside by the times. . . . [China] must firmly use Marxism to *occupy* the online [space, and] grasp

---

[11] Andrew Futter, '*Cyber' Semantics: Why We Should Retire the Latest Buzzword in Security Studies*, 3 J. CYBER POL'Y, 201, 205 (2018). The expression "ICT security" in lieu of the original "information security" has been preferred, since the chosen translation may better identify the scope of the issue at stake. Arguably, "information" is even broader than "ICT", because it refers to processes of governance and diplomacy which do not necessarily need any technological means or mediation to be employed or pursued. Accordingly, in the specific context of cybersecurity negotiations, "information" is probably best translated into English as "ICT". On the broad meaning of "information security" in diplomatic bureaucratese, see the examples provided in Tim Maurer & Robert Morgus, *Compilation of Existing Cybersecurity and Information Security Related Definitions*, 32–37, NEW AMERICA (Oct. 2014), https://www.giplatform.org/sites/default/files/Compilation%20of%20Existing%20Cybersecurity%20and%20Information%20Security%20Related%20Definition.pdf.

[12] Samuele Dominioni, *Multilateral Tracks to Tackling Cybercrime: An Overview*, ITALIAN INST. FOR INT'L POLITICAL STUDIES (July 16, 2018), https://www.ispionline.it/en/pubblicazione/multilateral-tracks-tackling-cybercrime-overview-20962.

[13] Johan Lagerkvist, *The Legitimacy of Law in China: The Case of "Black Internet Cafés"*, *in* MAKING LAW WORK: CHINESE LAWS IN CONTEXT 267, 285 (Mattias Burell & Marina Svensson eds., 2011).

[14] *See* Sarah McKune & Shazeda Ahmed, *The Contestation and Shaping of Cyber Norms: Through China's Internet Sovereignty Agenda*, 12 INT'L J. COMM., 3835, 3843 (2018); Suisheng Zhao, *The Ideological Campaign in Xi's China: Rebuilding Regime Legitimacy*, 56 ASIAN SURVEY 1168, 1179–1181 (2016).

[15] Jing Wu & Guoqiang Yun, *From Modernization to Neoliberalism? How IT Opinion Leaders Imagine the Information Society*, 80 INT'L COMM. GAZETTE 7, 8 (2018).

leadership power in online ideology work."[16] Conflict-wise, this novelty pertains to the so-called "Revolution in Military Affairs."[17] Politically speaking, in a globe "where countries wanting deep economic integration globally cannot hope to achieve all three goals of globalization, national sovereignty, and democracy,"[18] "[t]here is an enormous disconnect between the cyber realities of today and the theories of the twentieth century, which continue to guide national policy and international relations."[19] State institutions make "efforts to evade sovereignty issues by cooperating informally or extralegally," [20] and when lawmaking cannot be circumvented, preferences are given to informal fora and outcomes. China and the Eastern context more generally take the validity of these remarks to an even higher extent: A new wave of Confucianist legal thinking sustains an idea of law that announces a superficial curtain of "legitimacy and order" which only moral persuasion can bring to have any impact on societal attitudes and behaviors.[21] Confucianism tends to appear in awe of a kind of normativity which "seeks primarily to persuade and not to oblige,"[22] but this does not mean that such a persuasion may not assume fairly confident, assertive, or even verbally violent forms, [23] especially when matched with Western demands or faced with international pressure. International value partisanship over the conception of "sovereignty" has possibly

---

[16] Rogier J.E.H. Creemers, Paul S. Triolo & Graham Webster, *Translation: China's New Top Internet Official Lays Out Agenda for Party Control Online*, NEW AMERICA (Sept. 24, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-chinas-new-top-internet-official-lays-out-agenda-for-party-control-online/ (emphasis added).

[17] United Nations Inst. for Disarmament Research (UNIDIR), *Developments in the Field of Information and Telecommunications in the Context of International Security*, at 2 (Aug. 26, 1999).

[18] Hwa Ang Peng & Natalie Pang Lee San, *Globalization of the Internet, Sovereignty or Democracy: The Trilemma of the Internet Governance Forum*, 4 REVUE FRANÇAISE D'ÉTUDES AMÉRICAINES 114, 116 (2012).

[19] Nazli Choucri & Daniel Goldsmith, *Lost in Cyberspace: Harnessing the Internet, International Relations, and Global Security*, 68 BULL. ATOMIC SCIENTISTS 70, 75 (2012).

[20] MICHAEL ROSS FOWLER & JULIE MARIE BUNCK, LAW, POWER, AND THE SOVEREIGN STATE: THE EVOLUTION AND APPLICATION OF THE CONCEPT OF SOVEREIGNTY 158 (1995).

[21] Wen-Yeu Wang & Yen-Lin Agnes Chiu, *The Defining Characteristics of the Legal Family in East Asia*, *in* CODIFICATION IN EAST ASIA: SELECTED PAPERS FROM THE 2ND IACL THEMATIC CONFERENCE 3, 7 (Wen-Yeu Wang ed., 2014).

[22] H. PATRICK GLENN, LEGAL TRADITIONS OF THE WORLD: SUSTAINABLE DIVERSITY IN LAW 304 (2007).

[23] *See generally* Maria Repnikova & Kecheng Fang, *Authoritarian Participatory Persuasion 2.0: Netizens as Thought Work Collaborators in China*, 27 J. CONTEMP. CHINA 763 (2018).

never been as intense as today, particularly with regards to still underregulated policy domains.

The cyber world *per se* is a value-neutral, non-partisan one, since it can be the terrain of freedom and censorship, regime propaganda and revolutionary forces alike.[24] As far as the law is concerned, there are of course numerous sub-fields involved in the debate, ranging from the protection of trade secrets from cyber-attacks in intellectual property law, to the right to self-defense in international security law; from the limits of content filtering, to the performance of commercial transactions, and so forth. Attempts to use law as a tool to mediate between the governors and the governed in cyberspace show at times paradoxical facets.[25] Because of this, before entering into detailed negotiations on each of those sub-fields at the international level, the international community needs to find a common understanding on a number of fundamental, overarching, and cross-cut principles. It is widely acknowledged that NATO allies on the one side and Russia and China on the other are leading their own campaigns, underpinned by their own ambitions and values. More specifically, only Washington among the three major players (US, Russia, China) has ratified the beacon[26] cyber treaty to date—the Budapest Convention—but the US keeps behaving anarchically as a free rider, and the other two powers have built their own discursive alternatives.[27] What is more, India, for its part, "has not ratified the . . . Convention[,]which it considers a US-driven project prepared without any consultation with a broader international community."[28] There is no contention that Russia, China and India

---

[24] Choucri & Goldsmith, *supra* note 19, at 76. *See also* Thomas Schultz, *Carving up the Internet: Jurisdiction, Legal Orders, and the Private/Public International Law Interface*, 19 EUR. J. INT'L L. 799, 802 (2008).

[25] ROSTAM JOSEF NEUWIRTH, LAW IN THE TIME OF OXYMORA: A SYNAESTHESIA OF LANGUAGE, LOGIC AND LAW 73 (2018).

[26] Since its ratification, this treaty has become outdated. *See* KENNEDY G. GASTORN, ASIAN-AFRICAN LEGAL CONSULTATIVE ORG., RELEVANCE OF INTERNATIONAL LAW IN COMBATING CYBERCRIMES: CURRENT ISSUES AND AALCO'S APPROACH 6 (2017), *available at* http://www.aalco.int/WIC%20-%20%20Cybercrimes%20-%2027.12.17.pdf.

[27] JOSEPH SAMUEL NYE, JR., GLOB. COMM'N ON INTERNET GOVERNANCE, THE REGIME COMPLEX FOR MANAGING GLOBAL CYBER ACTIVITIES 10 (2014) ("The Budapest [C]onvention['s] . . . breadth has been limited by its origins in Europe. Many post-colonial countries and authoritarian countries such as Russia and China object to obligations that they see as intrusions on their sovereignty as well as the European origin of the norms.").

[28] PATRYK PAWLAK, INT'L AFFAIRS INST., EU-INDIA COOPERATION ON CYBER ISSUES: TOWARDS PRAGMATIC IDEALISM? 9 (2016).

shall be considered "critical states," "without which the achievement of the substantive norm goal is compromised."[29]

In this framework, the position of New Delhi as a potential mediator and negotiating bridge[30] to tip the balance towards one of these two major blocks has gone understudied. Indeed, someone has posited that India, as a "swing state,"[31] needs to "decide which group of states to align with or opt for a combination of the two approaches."[32] If India prefers aligning with the Russian-Chinese values, it would work with its SCO partners at consolidating their stances and upholding them internationally. By contrast, if it opts for a combination, it would attempt to close the gaps between the blocks in wide multilateral fora such as the UN. In the highly unlikely, but not impossible,[33] event that India decides to overtly join the Western approach, it would operate mainly within regional organizations whose membership encompasses India, the US, and the EU. In the first case (alignment with Russian-Chinese stances), the NATO-

---

[29] Martha Finnemore & Kathryn Sikkink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887, 901 (1998).

[30] Alex Grigsby, Glob. Comm'n on the Stability of Cyberspace, *Overview of Cyber Diplomacy Initiatives*, *in* BRIEFINGS TO THE GLOBAL COMMISSION ON THE STABILITY OF CYBERSPACE FOR THE FULL COMMISSION MEETING 6, 15 (2017), *available at* https://cyberstability.org/wp-content/uploads/2017/12/GCSC-Briefings-from-the-Research-Advisory-Group_New-Delhi-2017.pdf.

[31] MIRKO HOHMANN & THORSTEN BENNER, GLOB. PUB. POLICY INST., GETTING "FREE AND OPEN" RIGHT: HOW EUROPEAN INTERNET FOREIGN POLICY CAN COMPETE IN A FRAGMENTED WORLD 32 (2018); ANGEL PASCUAL-RAMSAY ET AL., ZURICH INS. GRP., RISK NEXUS – GLOBAL CYBER GOVERNANCE: PREPARING FOR NEW BUSINESS RISKS 15 (2015).

[32] ARINDRAJIT BASU, THE CTR. FOR INTERNET & SOC'Y, THE POTENTIAL FOR THE NORMATIVE REGULATION OF CYBERSPACE: IMPLICATIONS FOR INDIA 50 (2018).

[33] HOHMANN & BENNER, *supra* note 31, at 5 (correctly arguing that "European democracies can effectively engage key non-Western states that do not practice authoritarian digital policy. Countries like India and Brazil stand out as potential partners. Both have the capacity to shape norms and rules internationally"). India, as a free rider, acquires invaluable importance for both blocks. It is interesting to observe the synthesis of divergent narratives which takes place within the BRICS' "parallel order," whereby two authoritarian countries (China and Russia) are juxtaposed to more or less mature "democracies" (India, Brazil, and South Africa). *See* PETER VAN HAM, THE BRICS AS AN EU SECURITY CHALLENGE: THE CASE FOR CONSERVATISM 25 (2017); EYAL BENVENISTI & GEORGE W. DOWNS, BETWEEN FRAGMENTATION AND DEMOCRACY: THE ROLE OF NATIONAL AND INTERNATIONAL COURTS 46 (2017). This informal coalition's Working Group of Experts on Security in the Use of ICTs holds regular meetings, and takes cybersecurity very seriously, listing it as a priority concern. *See* Adriana Erthal Abdenur, *Can the BRICS Cooperate in International Security?*, 83 INT'L ORG. RESEARCH J. 73, 83 (2017).

SCO polarization would be left untouched or arguably widen. In the second case (combination), [34] such a polarization would be smoothened. In the third case (alignment with the West), one would no longer be able to talk of any true "SCO stance," as the stances within the SCO would get fragmented along the Russian-Chinese and Indian lines; such a scenario would unveil new balances between trust and mistrust which find explanation in the modern psychologic *Gestalttheorie*, positing that "the perception of all the individual constituents of any entity together constitutes something else and adds something new, a so-called 'Gestalt' (shape), to the sum of the single individual constituents."[35]

Ostensibly, Indian alliances follow an à-la-carte geometry, whereby "others may dream of playing an 'India card' in the East Asia geopolitical game . . . , [but] New Delhi does not see itself as a "card" in anyone's deck."[36] A historical reading of international law as *jus gentium* (i.e. *jus inter gentes*) widens its scope if compared to the classical doctrine of inter-state legal relations as to include (amid other configurations) the dialectic among "empires"—a sort of "*jus inter imperia*"—which are in the position of exercising political and economic supremacy over clusters of state territories or sovereignties.[37] If "the East" and "the West" stood as the two "imperial" poles of this concept (SCO thus representing "the Eastern empire"), India now comes in to complexify the chessboard and to turn this yet-stereotyped simplification into floating uncertainty.

---

[34] Rajeswari Pillai Rajagopalan, *India's Cyber and Space Security Policies*, *in* CHALLENGES AT THE INTERSECTION OF CYBER SECURITY AND SPACE SECURITY: COUNTRY AND INTERNATIONAL INSTITUTION PERSPECTIVES 22, 22 (Caroline Baylon ed., 2014) ("India has found an ideal blend of Western and Eastern approaches to cyber security. . . . Until several years ago, India viewed cyber security predominantly from a national security perspective, with its primary concern being the protection of critical infrastructure. Lately, however, it has increasingly emphasized social harmony and cohesion").

[35] Rostam Josef Neuwirth, *Governing Glocalization: "Mind the Change" or "Change the Mind"?*, https://www.umac.mo/fss/pa/4th_conference/doc/all%20paper/Session%201/Panel%201-1%20Globalization%20and%20the%20Role%20of%20Government/2%20Rostam%20J.%20Neuwirth/01_RJ_Neuwirth_(Governing_Glocalisation_-_Mind_the_Change)_21-10-2010.pdf.

[36] Ralph A. Cossa, *Security Dynamics in Asia, in* INTERNATIONAL RELATIONSHIPS OF ASIA 365, 373 (David Shambaugh & Michael B. Yahuda eds., 2014).

[37] CARL SCHMITT, THE NOMOS OF THE EARTH IN THE INTERNATIONAL LAW OF THE JUS PUBLICUM EUROPAEUM 211(G. L. Ulmen trans., 2006).

III. FORMAL AND INFORMAL LAWMAKING ON REGIONAL AND GLOBAL STAGES

> [A] host of […] factors contribute to the fact that legal positivism appears to be terribly outdated. A society marked by rapid technological development and the internationalization of commerce is difficult to reconcile with a mindset for which legal codes or commands appear to be the paradigmatic instances of law.[38]

Interstate obligations are increasingly being replaced by inter-organization coordination structures or interstate informal political arrangements and discussion platforms. From business and human rights to environmental protection and internal displacement, many international law areas are perpetually being shaped by soft standards and uncodified expectations, rather than binding obligations. The convenience thereof as opposed to hard provisions may be questioned on several grounds, as marginalized state and non-state actors indeed raise these questions in front of the relevant international fora. Powerful countries, on the other hand, do benefit from these trends by reducing the need for binding legal commitments and related lengthy negotiations on terminologies and values: Casual result-oriented agreements do not provide *opinio iuris* evidence useful to make the case for forming new customs;[39] in this respect, they differ from small countries' strategies to circumvent traditional lawmaking by seeking approval of resolutions within the United Nations General Assembly (UNGA)[40].

---

[38] Alexander Somek, *The Spirit of Legal Positivism*, 12 GERMAN L.J. 729, 730 n.5 (2011).

[39] Indeed, the potential binding force of new international customs is assessed by balancing state behaviours (which must be widespread, consistent, and relevant) with States' belief that said behaviours are the correct (i.e., legally accepted/acceptable) ones. Debates are inflamed on this issue. Although most scholarly writings confirm the necessity of these two elements, the required distribution between them—state practice and *opinio iuris*—remains an object of contention not yet definitely "settled" by the International Court of Justice.

[40] Although non-binding *de iure*, UNGA Resolutions are deemed by most publicists (and, on a case-by-case fashion, by the ICJ) as evidentiary sources for *opinio iuris* assessments. *See* Marko Divac Öberg, *The Legal Effects of Resolutions of the UN Security Council and General Assembly in the Jurisprudence of the ICJ*, 16 EUROPEAN J. INT'L L. 879 (2005); Samuel A.

In sum, informal coordination distances itself from familiar rules of public international law(making) more than infra-UN soft laws allow for.[41]

Along with the soft-hard law debate, another dichotomy is that between formal and informal lawmaking processes, whose importance grows in extremely technical negotiations like those on cyber governance. If the "cyber" dimension of state capabilities has contributed towards the redistribution of power across nations, with the rise of new "digital powerhouses" and a rapid spillover effect onto their real economies, then a lawmaking "informalization" process which "allows [for] the unofficial distinction between formally equal actors"[42] (informal inequality as opposed to formal equality) may help one read through the lines of such a transformation. Overall, informal lawmaking is distinct from the formal on a few main aspects related to its output and actors:

> [I]n traditional international lawmaking, the result is usually a treaty or any other classical source of international law. Output informality can be described as outcomes that do not fall under such sources, for example guidelines, standards or declarations. . . . Actors involved in international cooperation may be "informal" in the sense that they do not only engage traditional diplomatic actors (such as heads of state, foreign ministers or embassies), but also other ministries, domestic regulators, independent or semi-independent agencies . . . , sub-federal entities . . . or the legislative or judicial branches.[43]

An example in the West might well be the EU's Economic and Monetary Union, a *coordinative* set of policies and network of policymakers illustrating "one aspect of [globalised] neoliberal

---

Bleicher, *The Legal Significance of Re-Citation of General Assembly Resolutions*, 63 AMERICAN J. INT'L L. 444, 450 n.30 (1969); Anthea Elizabeth Roberts, *Traditional and Modern Approaches to Customary International Law: A Reconciliation*, 95 AMERICAN J. INT'L L. 757, 758 (2001).

[41] BENVENISTI & DOWNS, *supra* note 33, at 43–44.

[42] Cristopher Daase, *The ILC and Informalization*, *in* PEACE THROUGH INTERNATIONAL LAW: THE ROLE OF THE INTERNATIONAL LAW COMMISSION 179, 180 (Georg Nolte ed., 2009).

[43] Jan Maria Florent Wouters & Dylan Jan Werner Arnold Geraets, *The G20 and Informal International Lawmaking, in* INFORMAL INTERNATIONAL LAWMAKING: CASE STUDIES 19, 21 (Ayelet Berman et al. eds., 2012).

ideology: The 'cult of the expert,' leading to the transfer of power from accountable ministers to unaccountable technocrats. . . . *Liberalisation* has . . . brought in its wake an inevitable degree of *privatisation*."[44] Consistent with these criteria, one may observe a proliferation of informal settings for negotiations on cyber issues, priming accountability concerns due to their technocratic nature.[45] In order for international talks to keep pace with the latest ICT developments and technicalities, the "unrepresentative input"[46] of subject experts at the highest negotiating levels seems unavoidable,[47] and arguably it should become even more significant than it is now.[48] Only democratic states might have accountability problems here, because authoritarian states are not accountable to their "citizens" anyway. While informal networks lack accountability, they are relatively more effective in terms of their output legitimacy.[49] Both are important concerns and neither should completely overshadow the other.[50] The Asian diplomatic machinery—especially in East Asia—has been generally wary of formal regional organizational arrangements, while more recently embracing a multi-layered reality built on formally established organizations which are complementary, thus *not* alternative, to a deeper informal inter-state structure.[51] Lastly, regardless of the formal or informal negotiating settings and procedures, international organizations are by their nature reluctant to answer to the member

---

[44] DANNY NICOL, THE CONSTITUTIONAL PROTECTION OF CAPITALISM 107 (2010).

[45] Leonard F.M. Besselink, *Informal International Lawmaking: Elaboration and Implementation in the Netherlands, in* INFORMAL INTERNATIONAL LAWMAKING: CASE STUDIES 97, 138 (Ayelet Berman et al. eds., 2012).

[46] Pierre M. Horna, *Can Accountability and Effectiveness Go Hand in Hand? Lessons from Two Latin American Competition Networks, in* INFORMAL INTERNATIONAL LAWMAKING: CASE STUDIES 313, 320 (Ayelet Berman et al. eds., 2012).

[47] As to the financial markets, it might be slightly different. *Cf.* Shawn Donnelly, *Informal International Lawmaking: Global Financial Market Regulation, in* INFORMAL INTERNATIONAL LAWMAKING: CASE STUDIES 179, 186–87 (Ayelet Berman et al. ed., 2012).

[48] INDEP. COMM'N ON MULTILATERALISM & INT'L PEACE INST., THE IMPACT OF NEW TECHNOLOGIES ON PEACE, SECURITY, AND DEVELOPMENT 15 (2016).

[49] Luca Corredig, *Effectiveness and Accountability of Disaster Risk Reduction Practices: An Analysis through the Lens of IN-LAW, in* INFORMAL INTERNATIONAL LAWMAKING: CASE STUDIES 471, 497 (Ayelet Berman et al. ed., 2012).

[50] Horna, *supra* note 46, at 344.

[51] Robert Ayson, *Formalizing Informal Cooperation?, in* EFFECTIVE MULTILATERALISM: THROUGH THE LOOKING GLASS OF EAST ASIA 196, 196–97, 202 (Jochen Prantl ed., 2013).

states' citizens, and subject to the partisan pressure of NGOs and other hybrid transnational civil society actors,[52] in a context where "bureaucrats become powerful only by making themselves appear powerless."[53] This creates an almost insurmountable dilemma when it comes to isolating the political and legal contribution of each party to a certain policy negotiated within the international organization but concerned and exported externally in broader assemblies in representation of said organization.

One might think that an informal lawmaking pattern would represent a resourceful strategy for countries which, prior to colonization, followed oral or other unofficial lawmaking paths; put differently, the preference for informal lawmaking within an organization would benefit the members of that organization with a pre-colonial past built on legal informality. Such a legacy may assist them in framing their concerns more effectively in a flexible context. However, while some scholars suggest this might be an argument for the formation of international customs,[54] no evidence or research confirms or at least supports this link. Drawing a parallelism with linguistic anthropology, "the only universal distinction between oral and literary traditions is the historical anteriority of the first to the second. Beyond this obvious observation, it is pointless to insist on any universalizing definitions for the 'oral' of 'oral tradition.' 'Oral tradition' [depends] on the concepts of 'written tradition' . . . In cultures that do not depend on the technology of writing [*grámmata*], the concept of "orality" [*phōnḗ*] is meaningless."[55]

---

[52] Eyal Benvenisti, *Upholding Democracy Amid the Challenges of New Technology: What Role for the Law of Global Governance?,* 29 EUROPEAN J. INT'L L. 9, 15, 48 (2018). The same is true in terms of the identification and implementation of customary rules. Andreas L. Paulus & Matthias Lippold, *Customary Law in the Postmodern World (dis)Order*, 112 AM. J. OF INT'L L. 308, 312 (2018).

[53] MICHAEL BARNETT & MARTHA FINNEMORE, RULES FOR THE WORLD: INTERNATIONAL ORGANIZATIONS IN GLOBAL POLITICS 69 (2004).

[54] Brian D. Lepard, *"Customary International Law: A Third World Perspective": Reflections in Light of an Approach to CIL Based on Fundamental Ethical Principles*, 112 AM. J. INT'L L. 303, 305 (2018).

[55] Gregory Nagy, *Performance and Text in Ancient Greece*, CTR. FOR HELLENIC STUDIES AT HARVARD UNIV. (2010), https://chs.harvard.edu/CHS/article/display/3626.

IV. RUSSIA, CHINA AND THE TRADITIONAL SCO POSTURE

> Cyber "war" is an area of great, public concern, and several proposals have been made to limit, or even to prohibit, cyber warfare. Russia proposed several years ago that all forms of cyber warfare be outlawed. China refused to accept so sweeping a restriction, viewing cyber warfare as an arena in which it could be successful in competing with the U.S. and other militarily powerful states. The U.S. for years indicated it was uninterested in even discussing limitations on cyber warfare. Military officials assigned leading roles in developing U.S. cyber capacities in fact announced their intent to "dominate" cyberspace. The U.S. has created a Cyber Command, reflecting its view that cyber space is a new theater for national security activities analogous to the ground, sea, or air theaters of operations.[56]

"[T]he SCO presents itself as a new-style regional organization promoting mutual trust and regional cooperation that, unlike Western counterparts, does not interfere in the sovereignty of its [M]ember [S]tates by imposing […] political conditions."[57] With the steady decline of Japanese economic and diplomatic influence, the SCO has gained momentum as a platform connecting the major Asian powers. Up to June 2017, its membership was limited to China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan. One year after its foundation rooted in Central Asia,[58] the SCO was

---

[56] Abraham D. Sofaer, David Clark & Whitfield Diffie, *Cyber Security and International Agreements* (2010), 191–192, https://www.nap.edu/read/12997/chapter/13.

[57] Alexander A. Cooley, *Central Asia's Inside-Out Foreign Economic Relations, in* THE OXFORD HANDBOOK OF THE INTERNATIONAL RELATIONS OF ASIA 241, 249 (Saadia M. Pekkanen et al. eds., 2014).

[58] M. Taylor Fravel, *Territorial and Maritime Boundary Disputes in Asia*, *in* THE OXFORD HANDBOOK OF THE INTERNATIONAL RELATIONS OF ASIA 525, 540

already keen on projecting an image of openness and inclusiveness, as well as constructive availability for shaping the international community through normative consensus-building to be reached within the most appropriate venues; its narrative on transnational terrorist activities stands as exemplary in this respect:

> Effective steps will be taken in the SCO framework aimed at the implementation of the Shanghai Convention on Combating Terrorism, Separatism and Extremism. . . . Of urgent importance is establishing the mechanism of mutual information and search for common points of view on foreign policy issues of mutual interest, *inter alia*, in the framework of international organizations and fora, including the UN. . . . [T]he SCO is neither a bloc, nor a closed alliance, is not directed against any individual countries or groups of states and is open for broad cooperation with other states and international associations in accordance with the purposes and principles of the UN Charter and the norms of international law, on the basis of regard for mutual interests and of the commonality of approaches to dealing with regional and global problems.[59]

Motivated by the intent of "[p]reventing the use *or threatened use* of local *and global* computer networks for purposes of terrorism," [60] the SCO was fully determined not to remain marginalized in the international debates on information security and technological development. Interestingly, five years since its creation, it portrayed its stances in a truly open way, up to mentioning the Universal Declaration of Human Rights [61] and

---

(Saadia M. Pekkanen et al. eds., 2014); *Cf.* Niklas Swanström, *Central Asia and China's Security Policy*, *in* ROUTLEDGE HANDBOOK OF CHINESE SECURITY 229, 235–236 (Lowell Dittmer & Miles Maochun Yu eds., 2015).

[59] Declaration by the Heads of the Member States of the Shanghai Cooperation Organisation, Saint Petersburg, June 7, 2002, *available at* http://eng.sectsco.org/load/193445.

[60] Concept of Cooperation Between SCO Member States in Combating Terrorism, Separatism, and Extremism art. III(14), *available at* https://www.fidh.org/en/issues/terrorism-surveillance-and-human-rights/Concept-of-Cooperation-Between-SCO (emphasis added).

[61] Strikingly, "China has made a great play of its adherence to the Universal Declaration, and has published a white paper on its citizens' freedom to use the Internet." CHRISTOPHER T. MARSDEN, INTERNET CO-REGULATION: EUROPEAN

"recognizing that ICTs have created a significant potential for the development of human capabilities and full realization of human rights and freedoms."[62] This is obviously quite far a language from the one we are used to nowadays, centered on securitization and limitations on freedom, as well as subordination of human rights to the rhetoric of state, and not even regime, survival.[63] Nonetheless, the same document does not miss the opportunity to highlight that "the threat of the ICT use for criminal, terrorist and military and political purposes incompatible with maintenance of international security can be realized both within the civilian and military fields and cause serious political and socio-economic impacts on individual countries, regions and the world as a whole, and destabilization of public life within a state."[64]

The landmark SCO manifesto on information security comes three years later, eventually in the form of a formal intergovernmental agreement; it shall not question other treaty obligations of its members,[65] and employs Chinese and Russian as working languages for its implementation. *Prima facie*, it looks like

---

LAW, REGULATORY GOVERNANCE AND LEGITIMACY IN CYBERSPACE 235 (2011).

[62] Statement by the Heads of Member States of the Shanghai Cooperation Organisation on International Information Security, Shanghai, June 15, 2006, *available at* http://eng.sectsco.org/load/197770/.

[63] MARCEL DE HAAS, THE SHANGHAI COOPERATION ORGANISATION AND THE OSCE: TWO OF A KIND? 253 (2007), *available at* https://www.clingendael.org/sites/default/files/pdfs/20071100_cscp_art_haas.pdf . Specifically, Chinese government "conceptualized human rights as the Party-state's ruling capacity in regulating market order, providing social security and public services, instituting legal-procedural justice, *and shaping global governance*. The idea of human rights as the state's ruling capacity is consonant with, and plausibly conducive to, the Party-state's pursuit of the neoliberal mode of socio-economic *development*. The rights-as-threat conception and the rights-as-capacity proposition have co-existed with each other, forming a dualistic bastion of ideational support for the CCP's authoritarian rule" Titus C. Chen & Chia-hao Hsu, *Double-Speaking Human Rights: Analyzing Human Rights Conception in Chinese Politics (1989–2015)*', 27 J. CONTEMPORARY CHINA 534, 552 (2018) (two emphases added).

[64] Statement by the Heads of Member States of the Shanghai Cooperation Organisation on International Information Security, *supra* note 62.

[65] Agreement Between the Governments of the Member States of the Shanghai Cooperation Organisation on Cooperation in the Field of International Information Security art. 8, Yekaterinburg, June 16, 2009. Both the original Russian version and an unofficial English translation of this Agreement are reported in Theresa Hitchens and Nilsu Gören, *International Cybersecurity Information Sharing Agreements*, 26–47, CENTER FOR INT'L AND SECURITY STUD. UNIVERSITY MD. (Oct. 2017), http://www.cissm.umd.edu/sites/default/files/Cyber%20information%20sharing%20agreement%20report%20-%20102017%20-%20FINAL.pdf.

a non-belligerence and mutual-assistance pact among states which should share information with each other and refrain from attacking cyber infrastructures of other members.[66] Among other concepts, and implicitly referring to the United States and its NATO allies, it advances the fear of a "use of the dominant position in the information space to the detriment of the interests and security of other States,"[67] together with that arising from the "dissemination of information harmful to socio-political and economic systems, as well as the spiritual, moral, and cultural spheres of other States."[68] The agreement calls on parties to assist the internationalization of cyber governance worldwide by "elaborating collective measures regarding development of norms of international law to curb the proliferation and employment of information weapons that endangers national defense capabilities and public security," [69] which is exactly what the SCO has tried to pursue in the years to come. It has indeed codified a proposal submitted to the United Nations, and, despite Western resistance and general skepticism against the proposal,[70] it will persist in its attempt of upholding its stances before the international community.[71]

The proposal took the form of a "Code of Conduct" that was open to subscription by all states on a voluntary basis, and was presented in two versions distanced by four years. The first version was signed by China, Russia, Tajikistan and Uzbekistan, and contains several interesting provisions.[72] As demonstrated in the following list of examples, these provisions generate substantial doubts and uncertainties as to their effectiveness:

- "Not to use information and communications technologies, including networks, to carry out hostile

---

[66] *Id.* at art. 4.
[67] *Id.* at art. 2(4).
[68] *Id.* at art. 2(5).
[69] *Id.* at art. 3(3).
[70] Martha Finnemore & Duncan B. Hollis, *Constructing Norms for Global Cybersecurity*, 110 AMERICAN J. INT'L L. 425, 439 n.86 (2016); Alex Grigsby, *Will China and Russia's Updated Code of Conduct Get More Traction in a Post-Snowden Era?*, COUNCIL ON FOREIGN RELATIONS (Jan. 28, 2015), https://www.cfr.org/blog/will-china-and-russias-updated-code-conduct-get-more-traction-post-snowden-era.
[71] Development Strategy of the Shanghai Cooperation Organisation Until 2025, Dushanbe, September 12, 2014.
[72] Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan to the U.N., Letter dated Sept. 12, 2011 from the Permanent Reps. of China, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/66/359 (Sept. 14 2011).

activities or acts of aggression" (although hybrid warfare represents today's reality in most conflicts);

- "to cooperate . . . in curbing the dissemination of information that incites terrorism, secessionism or extremism or that undermines other countries' political, economic and social stability, as well as their spiritual and cultural environment" (such a scope seems extremely broad);
- "to ensure the supply chain security of information and communications technology products and services, in order to prevent other States from using their resources, critical infrastructures, core technologies and other advantages" (in this case, it is difficult to foresee any concrete consequence for Parties turning out to be unable to ensure such a high level of protection);
- "[t]o reaffirm all the rights and responsibilities of States to protect . . . their information space and critical information infrastructure from threats, disturbance, attack and sabotage" (whereas these "rights" provide states with substantial room for maneuver, the related—home and mutual—"responsibilities" place on them a burden not to be underestimated);
- "[t]o promote the establishment of a multilateral, transparent *and democratic* international Internet management system" (the detailed functioning of which may require decades of discussions);[73]
- "[t]o assist developing countries in their efforts to enhance capacity-building on information security" (what kind of assistance is required? And is China to be treated as a "developing country"?);
- "to . . . promote the important role of the United Nations in formulating international norms" (not necessarily

[73] *Cf*. Qingdao Declaration of the Council of Heads of State of the SCO, Section II, June 10, 2018, *available at* http://www.iri.edu.ar/wp-content/uploads/2018/09/a2018eurasiaDoc2QingdaoDeclaration.pdf. Written almost one decade later, the Declaration states that "all states should participate equally in Internet development and governance. A governing organisation established to manage key internet resources must be international, more representative and democratic." The Declaration proceeds further in the rhetoric of openness by proposing explicitly an egalitarian say in Internet governance for all members of the international community. This document is not to be mistaken for the *Qingdao Declaration on the Potential of ICT* following a conference organized by the Chinese National Commission for UNESCO in May 2015.

> binding, although this would be the Russian and arguably Chinese preference); and
>
> - "[t]o settle any dispute resulting from the application of the [C]ode through peaceful means." (then, is the use of force always *a priori* prohibited?)

As evidenced by this scrutiny, numerous doubts arise from a highly superficial and loosely-worded text. This is why a second ameliorated version was issued four years later,[74] this time undersigned by Kazakhstan and Kyrgyzstan as well. The most novel aspect of this draft is probably its Article 7, wherein States are requested to:

> [R]ecognize that the rights of an individual in the offline environment must also be protected in the online environment; to fully respect rights and freedoms in the information space, including the right and freedom to seek, receive and impart information, taking into account the fact that the International Covenant on Civil and Political Rights ([Art.] 19) attaches to that right special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) for respect of the rights or reputations of others; (b) for the protection of national security or of public order (*ordre public*), or of public health or morals.[75]

The SCO, most probably aware that resisting human rights expresses the intention of resisting the Western hemisphere's power dominance and technological primacy more broadly,[76] may have decided to turn to the human rights language with the aim of shortening the linguistic gap between the "Eastern" and "Western"

---

[74] Letter dated 9 January 2015 from the Permanent Reps. of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General, U.N. Doc. A/69/723 (Jan. 13, 2015).
[75] *Id.* at art. 7.
[76] The intentionality of such a resistance is historically ascertained for China. *See* ANN KENT, CHINA, THE UNITED NATIONS, AND HUMAN RIGHTS: THE LIMITS OF COMPLIANCE 51 (2013). *See also* HSIAO-CHI HSU, *The Limited Role of Naming and Shaming: International Human Rights Campaigns During the 2008 Beijing Olympics, in* INTERNATIONAL ENGAGEMENT IN CHINA'S HUMAN RIGHTS 98, 107–108 (Titus C. Chen & Dingding Chen eds., 2016).

ways to approach the law in theory and practice.[77] Put differently, employing the human rights discourse "as a form of legal imperialism"[78] is convenient to deliver the message in a West-friendly fashion—to "please the West," as one might phrase it—while leaving the substance untouched,[79] which is a normative strategy regularly opted for by nearly all countries in the West itself as well.[80] This strategy makes one's claims acceptable by the other party *in principle*, as deliberative democracy theorists would see it.[81] This is typical of organizations which "continuously manipulate legal materials and conceal their ambivalence or their radical subjectivity behind apparently formal or pragmatic responses, themselves calculated to reinforce the illusion of a solution that is founded in law."[82] Article 7 has been criticized for failing to mention the right to privacy,[83] a flagship aspiration for Western legal systems like those of the US and, more saliently, the EU.[84] One decade ago,

---

[77] ROSALYN C. HIGGINS, THEMES AND THEORIES: SELECTED ESSAYS, SPEECHES, AND WRITINGS IN INTERNATIONAL LAW 657 (2009) ("In some Asian countries, it has been said that human rights, as articulated in the Universal Declaration, elevates the individual and disembodies him from the community in which he exists. These countries perceive 'Western human rights,' with their emphasis on the individual, as encouraging the decline of moral authority and public order and as laying the foundation for the export of these evils into their own societies. . . . [T]here are in reality Western values and Asian values, with the former emphasizing the rights of the individual and the latter the interests of the community.").

[78] BILL BOWRING, THE DEGRADATION OF THE INTERNATIONAL LEGAL ORDER? THE REHABILITATION OF LAW AND THE POSSIBILITY OF POLITICS 135 (2008).

[79] Frank William La Rue (Special Rapporteur), *Rep. on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, U.N. Doc. A/HRC/17/27 (May 26, 2011) ("China, which has in place one of the most sophisticated and extensive systems for controlling information on the Internet, has adopted extensive filtering systems that block access to websites containing key terms such as 'democracy' and 'human rights.'").

[80] *See generally* Ben Wagner, Kirsten Gollatz & Andrea Calderaro, *Internet and Human Rights in Foreign Policy: Comparing Narratives in the US and EU Internet Governance Agenda*, ROBERT SCHUMAN CTR. FOR ADVANCED STUDIES (2014), http://cadmus.eui.eu//handle/1814/32433.

[81] IAN JOHNSTONE, THE POWER OF DELIBERATION: INTERNATIONAL LAW, POLITICS AND ORGANIZATIONS 16 (2011).

[82] NATHANIEL BERMAN, PASSION AND AMBIVALENCE: COLONIALISM, NATIONALISM, AND INTERNATIONAL LAW 35 (2012).

[83] KRIANGSAK KITTICHAISAREE, PUBLIC INTERNATIONAL LAW OF CYBERSPACE 13 (2017); PATRIK PAWLAK, EUROPEAN UNION INST. FOR SEC. STUDIES, A WILD WILD WEB? LAW, NORMS, CRIME AND POLITICS IN CYBERSPACE 2 (2017).

[84] *See, e.g.*, MAJA BRKAN & EVANGELIA PSYCHOGIOPOULOU, *The Court of Justice of the EU, Privacy and Data Protection: Judge-Made Law as a Leitmotif in Fundamental Rights Protectio*n, *in* COURTS, PRIVACY AND DATA PROTECTION

the worldwide regard for the EU Data Protection Directive 95/46/EC (the GDPR's predecessor) as a factual global standard attracted criticisms of Eurocentric regulatory imperialism by top offshore outsourcers like India and China.[85] There exists wide support for the applicability of human rights in cyberspace, starting indeed with the right to privacy as codified by Article 8 of the European Convention on Human Rights (ECHR) and Article 17 of the International Covenant on Civil and Political Rights (ICCPR).[86] Russia is a party to the ECHR, and as such is bound both territorially and extraterritorially not to violate that right, subject to the fact that the "extraterritorial application of human rights obligations requires effective control by the State concerned over the person affected (personal model) or the territory on which the operation takes place (spatial model)."[87] At the same time, anyone loyal to intellectual honesty cannot overlook the practical implications of, for example, the American overt and covert mass surveillance projects[88] for the concrete implementation and enjoyment of this right in the Western societies. At this point, one might wonder whether perpetuating the self-construed narrative of a "West" and an "East" in contraposition still makes sense,[89] although a few—admittedly important—features still differentiate these two blocs concerning ICT governance.

IN THE DIGITAL ENVIRONMENT 10 (Maja Brkan & Evangelia Psychogiopoulou eds., 2017).

[85] Sunni Yuen, *Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 COLUM. SCI. & TECH. L. REV. 72 (2008). This is particularly important for cybersecurity discourses, since (particularly Indian) "BPO [business process outsourcing] providers may be targeted as weak links in data security." Adrienne D'Luna Directo, *Data Protection in India: The Legislation of Self-Regulation*, 35 NW. J. INT'L L. & BUS. 5 n.15 (2017).

[86] China attached no reservations when it joined this Covenant, besides general provisions applicable to the Special Administrative Regions of Macao and Hong Kong under the "One Country, Two Systems" political configuration.

[87] Jeffrey Biller & Michael N. Schmitt, *Un-Caging the Bear? A Case Study in Cyber Opinio Juris and Unintended Consequences*, EUROPEAN JOURNAL OF INTERNATIONAL LAW: TALK! (OCT. 24, 2018), https://www.ejiltalk.org/un-caging-the-bear-a-case-study-in-cyber-opinio-juris-and-unintended-consequences/.

[88] WHITFIELD DIFFIE & SUSAN LANDAU, PRIVACY ON THE LINE: THE POLITICS OF WIRETAPPING AND ENCRYPTION 320–21 (2007).

[89] *See*, *e.g.*, Shaun BRESLIN & Silvia MENEGAZZI, *The Chinese Perspective on Global Order*, *in* STILL A WESTERN WORLD? CONTINUITY AND CHANGE IN GLOBAL ORDER: AFRICA, LATIN AMERICA AND THE "ASIAN CENTURY" 71, 78–79 (Sergio Fabbrini & Raffaele Marchetti eds., 2016) (perpetuating the contraposition between West and East). *Cf.* Evgeny MOROZOV, *Who's the true enemy of internet freedom – China, Russia, or the US?*, THE GUARDIAN (Jan. 3, 2015) (questioning the validity of such contraposition),

Beyond the usual rhetoric about the principles of territorial sovereignty[90] and non-interference in domestic affairs, the Sino-Russian axis[91] is concerned with cyberspace being a venue for competition over information resources between the US-EU alliance and the rest of the globe.[92] An Indian practitioner rightly noticed that sovereignty related to data generated by or passing through national ICT infrastructure is a key facet of international conversations on cybersecurity.[93] Russia and like-minded countries advocate for *content* control and governmental prerogatives over any cyber infrastructure lying within national physical borders. This helps ensure that their information infrastructure is not used for unwanted cyber activities and puts these countries in the position of asking the same of the broader international community. "The very term 'information security' preferred by China and Russia to the term 'cyber security' favored by the West is illustrative of the former's concern with content as opposed to the latter's focus on system integrity."[94] However, subscribing to these requests would place "an enormous legislative and administrative burden on States, [demanded not only to] supervise the legality of content within their own jurisdiction, but also ensure that it is considered inoffensive and non-hostile in the jurisdictions of all other [states]."[95] According to Russia, a state may only seek *lawful* access to specific parts of the information and communication infrastructure in the territory of

---

https://www.theguardian.com/commentisfree/2015/jan/04/internet-freedom-china-russia-us-google-microsoft-digital-sovereignty.

[90] For an instructive and updated comment on the application of this principle (and its rhetoric) to cyberspace activities performed by state actors, see Michael N. Schmitt, *In Defense of Sovereignty in Cyberspace*, JUST SECURITY (May 8, 2018), https://www.justsecurity.org/55876/defense-sovereignty-cyberspace/.

[91] Russia and China have indeed also finalised a "Joint Statement on Cooperation in Information Space Development", concerned with sovereignty and non-interference in the cyberspace. *See* KITTICHAISAREE, *supra* note 83, at 14. In linguistic terms, it is essential to note the frequent use of "non-interference" in lieu of "non-intervention" and vice versa, although the two expressions should *not* be deemed to be equivalent.

[92] KEIR GILES, *Russia's Public Stance on Cyberspace Issue at* 65, 2012 4TH INTERNATIONAL CONFERENCE ON CYBER CONFLICT (2012), *available at* https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6243966&tag=1.

[93] United Nations Inst. for Disarmament Research (UNIDIR), *Asia-Pacific Regional Seminar: Conference Report*, at 8 (2015), http://www.unidir.org/files/publications/pdfs/asia-pacific-regional-seminar-conference-report-en-623.pdf.

[94] PAUL MEYER, OUTER SPACE AND CYBERSPACE: A TALE OF TWO SECURITY REALMS 16 (2016). *See also* NYE, *supra* note 27, at 7; Grigsby, *supra* note 30, at 11.

[95] GILES, *supra* note 92, at 66.

another state which is employed for the perpetration of terrorist activities.[96] However, the Council of Europe's Budapest Convention is satisfied that "[a] Party may, *without the authorisation of another Party*, access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent *of the person who has the lawful authority to disclose the data* to the Party through that computer system." [97] Moscow deems the identification of such a person problematic,[98] not to mention the bypassing of the state's role in disclosure. Nonetheless, closer inspection suggests that such an omission may not be significant, as the consent of that person needs to both voluntary *and lawful*. Therefore, arguably, in compliance with the laws of the state where that person resides or of which they are a citizen. Moscow also has considerable concerns related to the "psychological war" that West-generated or West-mirroring content could knowingly or incidentally wage against the stability and social cohesion of the Russian population[99] if Russia were to adhere to the "free flow of information" doctrine advertised by the White House. Such promotion has been even more vigorous in the aftermath of the so-called 2003/2005 "Color Revolutions," the 2011 "Arab Spring,"[100] and the same year's Russian parliamentary elections.[101]

Although the cyber realm has proved too problematic in challenging the core foundations of international relations theory, the American rejection of more stringent rules may be expounded

---

[96] *Id.*

[97] Convention on Cybercrime art. 32(b), Nov. 23, 2001, E.T.S. 185 (emphasis added). It is worth keeping in mind that Russia is a party to the Council of Europe, not to be confused with European Union institutions.

[98] GILES, *supra* note 92, at 67.

[99] China fashions its objections in a similar vein. *See* Silvia Menegazzi, *China's Foreign Policy and Ideational Narratives: Key Trends and Major Challenges*, *in* UNDERSTANDING CHINA TODAY: AN EXPLORATION OF POLITICS, ECONOMICS, SOCIETY, AND INTERNATIONAL RELATIONS 175, 181 (Silvio Beretta et al. eds., 2017). SCO members agreed to include "mass psychological brainwashing to destabilize society" as part of the definition of "information warfare." Kai Ambos, *International Criminal Responsibility in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 118, 122 n.23 (Nicholas Tsagourias & Russell J. Buchan eds. 2015).

[100] GILES, *supra* note 92, at 71. *See also* STEPHEN ARIS, INT'L PEACE INST., SHANGHAI COOPERATION ORGANISATION: MAPPING MULTILATERALISM IN TRANSITION NO. 2 6 (2013), *available at* https://www.ipinst.org/wp-content/uploads/publications/ipi_e_pub_shanghai_cooperation.pdf.

[101] MARK A. BARRERA, THE ACHIEVABLE MULTINATIONAL CYBER TREATY – STRENGTHENING OUR NATION'S CRITICAL INFRASTRUCTURE 3 (2017), *available at* https://media.defense.gov/2017/Jun/19/2001764798/-1/-1/0/CPP_0003_BARRERA_MULTINATIONAL_CYBER_TREATY.PDF.

through realist lenses. With Washington being, and explicitly intending to be identified as, [102] the dominant power in cyber matters due to its unmatched, hegemonic technological capabilities, it receives no benefit from tiding-hands regulations [103] that run contrary to its competitive advantage. The Russian plea for arms control, against the backdrop of "more than 120 countries around the world [which] are working on or have already developed information weapons," [104] is fated to go unheard, even by its supposed Chinese partner.[105] Indeed, "cyberspace is an environment of persistent offense, where attacking is tactically and strategically more advantageous than defending," [106] and where traditional deterrence theories have limited applicability.[107] A scholar theorized that in the event of modern high-intensity confrontation, democratic

---

[102] *Id.* at 4.

[103] An example of tiding-hands regulations would be a global treaty regulating the fabrication, sale and usage of cyber weapons. *See* Louise Arimatsu, *A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations*, 4TH INT'L CONFERENCE ON CYBER CONFLICT (2012), https://ieeexplore.ieee.org/document/6243968; Cristian BARBIERI ET AL. *Non-proliferation Regime for Cyber Weapons. A Tentative Study*, INTERNATIONAL AFFAIRS INST. 18/3 (2018), *available at* http://www.iai.it/sites/default/files/iai1803.pdf. For a comparison with the US attitudes towards the Ottawa Convention banning landmines, see Paul N. Stockton & Michele Golabek-Goldman, *Curbing the Market for Cyber Weapons*, 32 YALE L. AND POL'Y REV. 239 (2013). For the dispute over the definition of "cyber weapon," see Prashant Mali, *Defining Cyber Weapon in Context of Technology and Law*, 8 INT'L J. CYBER WARFARE AND TERRORISM 43 (2018). Another example would be a provision prohibiting state-backed cyber-espionage as a means to steal military or industrial secrets from other countries. *See* Jack Landman Goldsmith, *How Cyber Changes the Laws of War*, 24 EUROPEAN J. INT'L L. 129, 135 (2013).

[104] Yury Barmin et al., *International Arms Control and Law Enforcement in the Information Revolution: An Examination of Cyber Warfare and Information Security*, 10 CONNECTIONS Q. J. 88 (2011).

[105] The secretive People's Liberation Army Cyber-Unit 61398 has "hacked into everything from the systems of hundreds of American companies, to U.S. government personnel records . . . , to a frightening number of plans for U.S. weapons systems, including the F-35 joint strike fighter, drones, nanotechnology, and electronic warfare systems. . . . China is also developing the capability to launch a serious cyber-attack on other countries' critical infrastructure, for example by shutting down an entire electricity grid." ANJA MANUEL, THIS BRAVE NEW WORLD: INDIA, CHINA, AND THE UNITED STATES 264 (2016). *See also* HEATHER HARRISON DINNISS, CYBER WARFARE AND THE LAWS OF WAR 55 (2012).

[106] Mariarosaria Taddeo, *Deterrence and Norms to Foster Stability in Cyberspace*, 31 PHIL. & TECH. 323, 325 (2018). Compare the irenic neoliberal approach in PHILIP N. HOWARD, PAX TECHNICA: HOW THE INTERNET OF THINGS MAY SET US FREE OR LOCK US UP (2015).

[107] Choucri & Goldsmith, *supra* note 19, at 71.

alliances are naturally fated to prevail *exactly because* of their faith in the "law of nations."[108] Nevertheless, it is difficult to apply this to cyber conflicts because the associated scale and extent of destruction are hardly comparable with those of the two world wars. "Insofar as cyber weapons depend on exploiting vulnerabilities in target software, the amount of damage that can be affected is often unpredictable[, and t]his inability to credibly threaten a specific magnitude of retaliation fundamentally undermines strategic deterrence."[109] Employing international law for deterrence and non-proliferation purposes in cyberspace may be complicated if not completely unfeasible. This is especially true when compared to other threats from weapons of mass destruction, like nuclear weapons.[110] Unlike nuclear weapons, cyber weapons may be developed fairly easily by private entities with little to no support by the state, at a relatively low price and incredible speed, all while causing disproportionally large damages. At the other end of the spectrum, "Russia and China have reason to distrust the use of cyber capabilities by the US owing to Washington's military superiority and considerable expertise in the cyber domain and the global Internet,"[111] especially given the aggressive rhetoric of the White House in its latest cyber-policy documents.[112] Certain rumored occurrences, such as Kremlin-backed Distributed Denial-of-Service (DDoS) attacks,[113] meddling in foreign elections,[114] and targeting of

---

[108] *See generally* MARC COGEN, DEMOCRACIES AND THE SHOCK OF WAR: THE LAW AS A BATTLEFIELD (2012).

[109] METTE EILSTRUP-SANGIOVANNI, *Why the World Needs an International Cyberwar Convention*, 31 PHIL. & TECH. 379, 390 (2017).

[110] *Cf.* MARY ELLEN O'CONNELL & LOUISE ARIMATSU, CYBER SECURITY AND INTERNATIONAL LAW MEETING SUMMARY (2017), *available at* https://www.chathamhouse.org/sites/default/files/public/Research/International%20Law/290512summary.pdf; Barmin et al., *supra* note 104, at 81; EILSTRUP-SANGIOVANNI, *supra* note 109, at 380.

[111] Eneken Tikk-Ringas, *International Cyber Norms Dialogue as an Exercise of Normative Power*, 17 GEO. J. INT'L AFF. 47, 53. *See also* Giovanni Salvini, *The Relations Between the People's Republic of China (PRC) and the United States (US)*, *in* UNDERSTANDING CHINA TODAY: AN EXPLORATION OF POLITICS, ECONOMICS, SOCIETY, AND INTERNATIONAL RELATIONS 95, 105 (Silvio Beretta et al. eds., 2017).

[112] NATIONAL CYBER STRATEGY OF THE UNITED STATES OF AMERICA (Sep. 21, 2018).

[113] O'CONNELL & ARIMATSU, *supra* note 110, at 4.

[114] KITTICHAISAREE, *supra* note 83, at 192; Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 30–67 (2018).

submarine cables,[115] may contradict the theory,[116] but, doctrinally speaking, Russian cyber operations are based on military defense and deception "aimed at preventing the negative effects of the spread of misinformation about the internal politics of Russia" rather than offence.[117] Hence, as an effort to hold a discursive leverage in the event of large-scale cyber conflicts, their attempt to rewrite the rules of the game appears perfectly reasonable. The "interstitial lawmaking" theorists,[118] however, warn that one must be cautious about what this rewriting truly entails. Rather than crafting a legal framework *ex novo*, it might evoke old rules, whose universal acceptance is taken for granted, and refashion them in unprecedented ways embedded with state doctrines. "[R]eferring to a set of norms Russia *considers* universally accepted deprives Russia of any responsibility for their articulation,"[119] whereas China seems ready to take on the honor and the burden of such articulation. Not astonishingly, Beijing makes no reference to the private sector in its strategies, which is considered one of the key pillars of the American approach[120] and the Indian business diplomacy.[121]

---

[115] KITTICHAISAREE, *supra* note 83, at 159–160.
[116] EILSTRUP-SANGIOVANNI, *supra* note 109, at 386.
[117] GILES, *supra* note 92, at 69–70.
[118] JOHNSTONE, *supra* note 81, at 48.
[119] Tikk-Ringas, *supra* note 111, at 53 (emphasis added).
[120] Choucri & Goldsmith, *supra* note 19, at 74. Some examples of the American approach are the network of NATO's Cooperative Cyber Defense Center in Tallinn, as well as the organizations affiliated to the CERT Coordination Center. *Id.* at 73.
[121] It is no accident that the 2017 Global Conference on Cyber Space took place in Delhi. *See* ACCESS PARTNERSHIP, NORMS FOR CYBERSECURITY IN SOUTH-EAST ASIA: POLICY OPTIONS FOR COLLABORATIVE SECURITY IN THE SOUTHEAST ASIAN REGION 12 (2017), *available at* https://www.accesspartnership.com/cms/access-content/uploads/2017/11/Access-Partnership-for-Web.pdf. For an Indian view on the event, see, for example, Chayanika Deka, *Issue Brief for the Global Conference on Cyber Space*, INDIAN COUNCIL ON WORLD AFFAIRS (Feb. 20, 2018), https://icwa.in/pdfs/IB/2014/GCCS2017IB20022018.pdf.

V. INDIA'S CONTRIBUTION TOWARDS A POSSIBLY NOVEL SCO APPROACH

> The issue of Internet governance should not be allowed to get bogged down in the divisive discussions of semantics.[122]

In June 2017, the SCO Members made the landmark decision of finally admitting India and Pakistan into the Organisation. "Russia welcomed the entry of India and Pakistan into the SCO as a way to diminish the outsized role of China's economic power within the group."[123] Meanwhile,"[f]or India, Russia serves as . . . the best possible hope of breaking the China-Pakistan axis[, as well as] the reimagining of Asia on its own terms rather than through a 'Western' prism."[124] That choice brought with it the long-lasting frictions between India and Pakistan and between Beijing and New Delhi, stemming from border disputes and more recently, the Belt and Road Initiative. [125] Nevertheless, Chinese President Xi Jinping underscored the need to build trust and solidarity at the regional level in order to overcome the greater uncertainty of global markets and governance.[126] It might also be argued that China and Russia were seeking normative convergence from the South: "To the extent that interpretive communities coalesce in International Organizations (IOs), the justificatory discourse there becomes more demanding. The parameters of acceptable argumentation are more apparent, deviation from those standards is easier to spot, and the cost of straying beyond accepted argumentative practices is felt more acutely."[127] In addition, India must have been regarded as a suitable norm exporter in the developing world through the pretentiously neutral channel of capacity-building. This is particularly relevant in the ICT sector, where the provision of technical assistance

---

[122] U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, Reply from the Government of India, 10, U.N. Doc. A/71/172 (July 19, 2016).
[123] RICK ROWDEN, GLOBAL POLITICAL ECONOMY BRIEF NO. 11: THE RISE AND RISE OF THE SHANGHAI COOPERATION ORGANISATION 7 (2018).
[124] Samir Saran, *Indian Contemporary Plurilateralism*, *in* THE OXFORD HANDBOOK OF INDIAN FOREIGN POLICY 622, 631–632 (David M. Malone et al. eds., 2015).
[125] ROWDEN, *supra* note 123, at 7.
[126] *Cf.* Martha Brill Olcott, *Central Asia: The End of the "Great Game"?*, *in* INTERNATIONAL RELATIONS OF ASIA 267, 284 (David Shambaugh & Michael B. Yahuda eds., 2014).
[127] JOHNSTONE, *supra* note 81, at 8.

transforms the recipient state into a dependent, and thus loyal, normative follower; aware of this, "[i]n [A]rt. 11 of the Code of Conduct member states confirm[ed] their commitment to assist developing countries to enhance their capacity in the field of information security."[128] India, as part of the SCO, represents simultaneously a recipient country and the necessary link between China and Russia on the one hand, and the "Third World" on the other, particularly in the Pacific region and with the English-speaking African countries.

During the speech he delivered a few minutes before the two countries joined the SCO, President Xi recalled that "security is the prerequisite for development. Without security, there will be no development to speak of. Recent acts of terrorism in this region show that the fight against the [terrorist, extremist, and separatist] forces remains a long and arduous task."[129] These remarks reflect the dissimilar sociological meaning attributed to "terrorism" by Eastern and Western countries: While for the latter it represents a threat *from the outside*, countries like China are obsessed with acts of rebellion and destabilization *from-within*.[130] A comprehensive rhetoric of the state has indeed been concocted since time immemorial[131] to sunder the "real Chinese", the *hanren*,[132] from the *hanjian*, the betrayers of the thoroughbred national ancestry to be persecuted and punished

---

[128] Zine Homburger, *The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace*, 33 GLOB. SOC'Y 224, 234 (2019).

[129] Xi Jinping, President of the People's Republic of China, Address at the 17th Meeting of Council of Heads of States of the Shanghai Cooperation Organisation (SCO) (9 June 2017).

[130] What might be read as a sociological construction, does in reality accurately reflect the situation on the ground: While China and Russia need to cope with internal separatist troubles (from Chechnya in Russia to the Chinese autonomous region of Xinjiang), the wider anti-terrorism projection of the United States extends to the policing of the whole planet. Nevertheless, China's so-called "Belt and Road Initiative" (previously known as the "One Belt, One Road Initiative") might relax this dichotomy, as Chinese business and telecommunication apparatuses would need (arguably for the first time) to venture in situations where directly facing exogenous terrorist threats seems unavoidable. YIWEI WANG, THE BELT AND ROAD INITIATIVE: WHAT WILL CHINA OFFER THE WORLD IN ITS RISE 90–92 (2016).

[131] YUN XIA, DOWN WITH TRAITORS: JUSTICE AND NATIONALISM IN WARTIME CHINA 3ff (2017).

[132] The descendants of the Han dynasty nowadays form *almost* 94% of the population of the "Greater China" region (roughly, the 92% of PRC's population—including its two Special Administrative Regions of Macao and Hong Kong—and the 96% of the Taiwanese one).

judicially and extrajudicially.[133] This helps explain the East's focus on national control juxtaposed to the West's liberal approach to content dissemination, whereas the United States, the EU, Japan, and Australia prefer to free the information flows, to then secretly monitor them by means of intelligence systems. More plainly, "letting any information come in" is the only way for the West to prevent possible terrorist threats *from external sources of concern*. President Xi subsequently reiterated Beijing's willingness to host once more the SCO joint counter-terrorism cyber exercise, and to assist the SCO "in speaking with one voice on international and regional issues," arguably including global cyber governance.[134] Remarkably, he has framed his commitments to security from a developmental perspective, which in international law terms one may understand as an attempt to claim a broader assertiveness of China's "right to development."[135] This is of no surprise, as China has consistently championed the global advocacy movement for the right to development to be recognized and upheld.[136] Such a right has unleashed fierce doctrinal debates, related not only to the extent

---

[133] Today, *hanjian* still may invariably include war traitors and the like, but also racial minorities. *See* Stephen John Hurley, Shame of a Nation: The Evolution of Hanjian since the Late Qing (May 3, 2012) (unpublished undergraduate honors thesis, College of William and Marry) (on file with W&M ScholarWorks), *available at* https://scholarworks.wm.edu/honorstheses/504.

[134] *Full text of Chinese President Xi's speech at 17th SCO Summit*, CHINA DAILY (June 9, 2017), http://www.chinadaily.com.cn/world/2017xivisitskazakhstan/2017-06/09/content_29691652.htm.

[135] In his speech, Xi pointed out that "[w]ithout cybersecurity there is no national security; without informatization, there is no modernization (没有网络安全就没有国家安全，没有信息化就没有现代化)." Paul S. Triolo et al., *Xi Jinping Puts "Indigenous Innovation" and "Core Technologies" at the Center of Development Priorities*, NEW AMERICA (May 1, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/xi-jinping-puts-indigenous-innovation-and-core-technologies-center-development-priorities/. *See also* An Baijie, *Xi: Security key to development*, CHINA DAILY (June 10, 2017), http://www.chinadaily.com.cn/china/2017-06/10/content_29692991.htm; Rogier Creemers et al., *Translation: Xi Jinping's April 20 Speech at the National Cybersecurity and Informatization Work Conference*, NEW AMERICA (Apr. 30, 2018), https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-xi-jinpings-april-20-speech-national-cybersecurity-and-informatization-work-conference/. For the official statement released by the Chinese Government on the "Right to Development," see *The Right to Development: China's Philosophy, Practice and Contribution (Full Text)*, STATE COUNCIL INFORMATION OFFICE (Dec. 2, 2016), http://www.scio.gov.cn/32618/Document/1534069/1534069.htm.

[136] Yuan Zhengqing et al., *China and the Remolding of International Human Rights Norms*, 38 SOCIAL SCIENCES IN CHINA 25, 37–38 (2017).

of this right, but also to its true existence.[137] The joint declaration released after the meeting built on the 2009 agreement in its purpose of continuing "to strengthen practical interaction in countering propaganda and justifications of terrorism, separatism and extremism in the media" and to "coordinate [the SCO Members'] efforts in order to resolve these tasks with the relevant countries, and regional and international organizations in bilateral and multilateral formats, including with the corresponding UN institutions."[138]

The ambiguous and somewhat cryptic information which were publicized from the SCO meetings makes it difficult to appraise how pivotal the Indian presence is towards redefined ICT security preferences and policy priorities. "Conventional IR approaches assume that change in IOs must be the result of changing demands of strongstates, but . . . getting any large bureaucracy, including international bureaucracies, to reform or respond to demands for change can be an exercise in frustration."[139] There is little doubt this holds true. However, this is far less verifiable for Eastern IOs which, unlike Western or Western-led ones, are not rigidly engineered with detached voting procedures. Where consensus takes primacy over mathematics, IOs' bureaucracy succumbs to member states' normative inputs in a less precisely measurable (that is, hardly severable among Members) but sounder-in-impetus fashion. [140] Since decisions within the SCO are taken by consensus, and

---

[137] *See*, *e.g.*, , IMPLEMENTING THE RIGHT TO DEVELOPMENT: THE ROLE OF INTERNATIONAL LAW, (Stephen P. Marks ed., 2008); Wouter Vandenhole & Paul Gready, *Failures and Successes of Human Rights-Based Approaches to Development: Towards a Change Perspective*, 32 NORDIC J. HUMAN RIGHTS 291 (2014); Paul Gready, *Rights-based approaches to development: what is the value-added?*, 18 DEVELOPMENT IN PRACTICE 735 (2008); Hannah Miller, *Rejecting "rights-based approaches" to development: Alternative engagements with human rights*, 16 J. HUMAN RIGHTS 61 (2017).

[138] Declaration of the Heads of State of the Shanghai Cooperation Organisation, Astana, June 9, 2017, *available at* http://eng.sectsco.org/load/297146/.

[139] BARNETT & FINNEMORE, *supra* note 53, at 8.

[140] Similarly, when it came to negotiating the ASEAN Charter, the less powerful countries lamented that "the retention of the principle of consensus in decision-making [for] being not progressive or forward-looking." TOMMY KOH, ROSARIO G. MANALO &WALTER WOON, THE MAKING OF THE ASEAN CHARTER 18 (2009). However, as long as States are in fact able to discuss fruitfully, allocating power to them is not a defeating strategy *per se*: It depends on how many countries join the forum, and how many among them shape its policies. In small-membership organizations like the SCO, where power is distributed among more than one party, consensus allows for exchange of views where all (or a significant proportion of) members are involved, whereas more (horizontally) participated IOs like the ASEAN may be held hostage by consensual decision-making schemes that pave the way for a hegemon to dictate the agenda.

cooperation is based on trust more than on laws,[141] normative tensions between India and the founders may witness tremendous repercussions.[142] On the one hand, a relatively recent document still endorses the traditional SCO stances as agreed in 2009 prior to the enlargement,[143] and therefore the Indian influence seems to be negligible. If this was in fact the case, the argument that the "growth and spread of international organizations ha[s] extended the executive command of the powerful states that [control] these institutions" would have retained its validity.[144] A closer look, however, unveils several notions on which India's contribution may be decisive. For instance, neither of the two SCO's Codes of Conduct, both of which were written before India joined SCO, endorsed the legality of anticipatory self-defense or preventive use of force in the cyberspace.[145] India, however, has traditionally adopted a different position on this issue:

> Most observers agree that states do not need to wait for the actual attack to commence, notwithstanding the fact that [Art. 51] UN Charter reads "if an armed attack occurs". There is also universal acknowledgment of the three prongs of the *Caroline* test: namely the necessity for the use of self-defence ("instant, overwhelming leaving no choice of means and no moment for deliberation"),

---

[141] Stephen Grainger, *The Shanghai Cooperation Organisation (SCO): Challenges Ahead and Potential Solutions*, GLOBAL SCIENCE & TECHNOLOGY FORUM (2012), *available at* https://ro.ecu.edu.au/ecuworks2012/160/.

[142] Rashid Qutbiddinovich Alimov, *The Shanghai Cooperation Organisation: Its Role and Place in the Development of Eurasia*, 9 J. EURASIAN STUD. 114, 116–17 (2018). Indeed, "China ha[d] been hesitant to admit India, arguing that the SCO [wa]s still too young to admit a large power like India. [Beijing was] concerned that India's admission would [have made] the organization's decision-making process much more complicated." VINOD K. AGGARWAL & MIN GYO KOO, *Trade Institutions in Asia*, *in* THE OXFORD HANDBOOK OF THE INTERNATIONAL RELATIONS OF ASIA 710 (Saadia Pekkanen et al. eds., 2014).

[143] *Development Strategy of the Shanghai Cooperation Organisation Until 2025*, 13 (Sept. 12, 2014).

[144] Benvenisti, *supra* note 52, at 13.

[145] The two are not perfect synonyms: "Even if the current collective security systems creates [sic] loopholes in which states are left undefended against potentially grave dangers, the immediacy element must be used to distinguish self-defence from preventive use of force. . . . [T]here is no 'preventive self-defence.' The term is a paradoxical construction. . . . One can refer to preventive use of force . . . but not to preventive self-defence." KINGA TIBORI SZABÓ, ANTICIPATORY ACTION IN SELF-DEFENCE: ESSENCE AND LIMITS UNDER INTERNATIONAL LAW 314 (2011).

> proportionality (the attack must not involve anything unreasonable or excessive) and imminence of the attack itself. The disagreement lies in how imminent the prospective attack must be. [In traditional warfare,] India's war doctrine permits the launch of pre-emptive operations in case there are continuing provocations *cumulatively* amounting to an "armed attack."[146]

Consequently, New Delhi may decide to shape the international community's stances on the transposition of this doctrine into the cyber dimension, under the cover of what Jacques Derrida would have identified as "democratic autoimmunity," expressed via the non-democratic preservation of democratic institutions.[147]

In order to make sense of a country's incumbent contribution (variable) within a consolidated organization (constant), it is often useful to introduce external controllers, such as the simultaneous behavior of that country within similar organizations.[148] In the case under scrutiny, one might look at India's identity as a party to the Commonwealth of Nations and the SAARC.[149] In its subject-

---

[146] Arindrajit Basu, *India Needs a Credible Deterrence Strategy for Cyberspace*, THE WIRE (Sept. 3, 2017), https://thewire.in/tech/india-needs-credible-deterrence-strategy-cyberspace (emphasis added).

[147] Michaele Ferguson, *Sovereignty, Democracy, Autoimmunity*, 12 EUR. LEGACY 487, 489 (2007); Daniel Matthews, *The Democracy To Come: Notes on the Thought of Jacques Derrida*, CRITICAL LEGAL THINKING (Apr. 16, 2013), http://criticallegalthinking.com/2013/04/16/the-democracy-to-come-notes-on-the-thought-of-jacques-derrida.

[148] In this case, "similarity" may be identified by type (e.g., NGOs, GOs, etc.), decision-making configuration (e.g., intergovernmental, supranational, confederate, etc.), as well as coefficient of membership homogeneity.

[149] Not to be confused with the Commonwealth of Independent States ("CIS"), also known as the "Russian Commonwealth" which includes Armenia, Azerbaijan, Belarus, Kazakhstan, Kyrgyzstan, Moldova, Russia, Tajikistan, and Uzbekistan. *See* Keith Crane et al., *Russian Investment in the Commonwealth of Independent States*, 46 *Eurasian Geography and Economics* 405, 406 n.3 (2005). The CIS will not be analysed here despite its rudimental attempts at cyber policing (refer, e.g., to its Dubai Action Plan 2015–2017), since it is described by most scholars as the paradigmatic exemplification of regionalism failure. *See*, *e.g.*, Paul Kubicek, *The Commonwealth of Independent States: An example of failed regionalism?*, 35 REV. INT'L STUD. 237 (2009); Richard Sakwa & Mark Webber, *The Commonwealth of Independent States, 1991–1998: Stagnation and Survival*, 51 EUROPE-ASIA STUD. 379 (1999); Mwita Chacha & Yoshiharu Kobayashi, *Migration and public trust in the Commonwealth of Independent States*, 28 REGIONAL AND FEDERAL STUD. 523, 525 (2018). Additionally, "[i]n the UN system, the CIS [M]ember [S]tates are split between two regional groups or voting blocs, making cooperation and co-ordination

specific declaration, the Commonwealth could not be farther from the SCO's traditional positions, starting from its emphasis on "voluntary norms of responsible state behavior," even though it committed itself to promote frameworks for the *applicability* (rather than the *application*) of international law, meaning that some degree of uncertainty on the convenience of the current international legal order still remains.[150] The Commonwealth also advocated for harmonized standards across its Members, possibly based on model laws, and considered "the potential for … coordination of common positions in international fora."[151] Nevertheless, the international outlook of this document seems tangential, as its Implementation Plan 2018-2020 does not mention any specific position to be lobbied for in any international forum.[152] The apparent preference for non-binding international regulation allowed India to agree on strengthening policy coordination on cyber matters with ASEAN, whose stances will be discussed in the next section.[153] Turning to the SAARC (which also incorporates Afghanistan, Bangladesh, Bhutan,

---

between the various national delegations slightly more difficult," with, for example, Russia in the Eastern European Group while Kazakhstan, Kyrgyzstan, Tajikistan, Turkmenistan and Uzbekistan are part of the Asia-Pacific one together with China and India. Flemming Splidsboel Hansen, *Do the CIS Member States Share Foreign Policy Preferences?*, 6 J. EURASIAN STUD. 69, 71 (2015).

[150] *Commonwealth Cyber Declaration*, ¶¶ 3–4, THE COMMONWEALTH (Apr. 20, 2018), https://chogm2018.org.uk/sites/default/files/Commonwealth%20Cyber%20Declaration%20pdf.pdf.

[151] *Id.* at ¶ 2.

[152] This Implementation Plan is not mentioned in academic literature, and can hardly be found in gray literature such as reports of relevant think-tanks; for example, no mention of it is made in the workshop report, *Cybersecurity in the Commonwealth: Supporting Economic and Social Development and Rights Online*, CHATHAM HOUSE (Oct. 4, 2018), https://chathamhouse.soutron.net/Portal/Default/en-GB/RecordView/Index/182669.

[153] This preference is in fact not explicit: according to the Indian delegation, "the issue of cyberwarfare, cyberdoctrines and their impact on international security should be discussed at all international forums. While rules of responsible State behaviour in cyberspace are still be [sic] agreed to, a common understanding on the confidence-building measures as enumerated in the 2015 report of the United Nations Group of Governmental Experts could be used for taking appropriate measures for capacity-building in the area of cybersecurity." U.N. Secretary-General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 11, U.N. Doc. A/71/172 (July 19, 2016). *See also Delhi Declaration of the ASEAN-India Commemorative Summit to Mark the 25th Anniversary of ASEAN-India Dialogue Relations*, ¶ 13 (Jan. 25, 2018), https://asean.org/storage/2018/01/Delhi-Declaration_Adopted-25-Jan-2018.pdf.

Maldives, Nepal, Pakistan, and Sri Lanka), India joined the other Members in attentively following the ICT developments as a means for poverty eradication.[154] Put differently, Delhi's traditional understanding of cyber technologies is grounded on economic emancipatory strains rooted in the non-traditional notion of "comprehensive security," known in the West as "human security," rather than a desire for spatial imperialism or economic domination.[155] Four years ago, on the wave of the international community's concerns about offline and online terrorist attacks, the SAARC listed the willingness "to establish a cybercrime monitoring desk" among its counterterrorism activities, and generally tabled its preference "for an early conclusion of a UN Comprehensive Convention on International Terrorism."[156] This is of particular interest here, as it may imply the Indian openness to a chapter on *cyber* terrorism within a comprehensive binding international counterterrorism treaty.[157] Notwithstanding this choice, it is hard to imagine where the line between cyber warfare and cyber terrorism might be drawn; needless to say, striving for new binding norms on

---

[154] *Tenth SAARC Summit Colombo Declaration*, 5 S. ASIAN SURV. 265, ¶¶ 9, 46, 69 (1998).

[155] TEPEKROVI KISO, INDIA'S FOREIGN POLICY TOWARDS SOUTH ASIA: RELEVANCE OF NORTH EAST INDIA 138 (2014). For the Chinese approach to the same concept of "comprehensive security", see Patricia M. Thornton, *China's Non-traditional Security*, *in* ROUTLEDGE HANDBOOK OF CHINESE SECURITY 64, 67 (Lowell Dittmer & Miles Maochun Yu eds., 2015).

[156] *Kathmandu Declaration*, SOUTH ASIAN ASSOCIATION FOR REGIONAL COOPERATION (Nov. 27, 2014), https://www.thedailystar.net/sites/default/files/upload-2014/gallery/pdf/kathmandu-declaration.pdf.

[157] Compare with the *BRICS Leaders Xiamen Declaration* whose scope is slightly wider: "We consider the UN has a central role in developing universally accepted [non-binding] norms of responsible state behavior in the use of ICTs to ensure a peaceful, secure, open, cooperative, stable, orderly, accessible and equitable ICT environment. . . . We emphasize the need to enhance international cooperation against terrorist and *criminal* misuse of ICTs . . . and recognize the need for a universal regulatory *binding instrument on combatting the criminal use of ICTs* under the UN auspices . . . We believe that all states should participate on an equal footing in the evolution and functioning of the Internet and its governance. . . ." ¶¶ 56–57 (Sept. 4, 2014), https://www.brics2017.org/english/documents/summit/201709/t20170908_2021.html (emphasis added). It shall be borne in mind that all these declarations are themselves non-binding, although they may be deemed strongly evidentiary of general policy orientations as they are reshaped over time. Both the "ASEAN Way" and the "BRICS Way" have been characterised in literature as shaped by informal arrangements often codified in non-binding agreements. *See* Alexandr Svetlicinii, *Global Fragmentation of Competition Law and BRICS: Adaptation or Transformation?*, *in* THE BRICS-LAWYERS' GUIDE TO GLOBAL COOPERATION 123, 138 (Rostam Josef Neuwirth et al. eds., 2017).

cyber terrorism whilst advocating soft rules on cyber warfare seems unwise and incoherent a policy.

Furthermore, India's approach to cyber security may be retrieved from its bilateral dialogues with Western countries and organizations. Interestingly, both India and the EU deem international law an important tool for making cyberspace a free and secure environment, although they feel the necessity to better clarify *how* current international laws are to be applied.[158]

VI. RUSSIA, CHINA, AND INDIA IN THE BROADER INTERNATIONAL CONTEXT

> The combined GDP measured in purchasing power parity of countries such as India and China is already greater than that of the United States. And a similar calculation with the GDP of the BRIC countries – Brazil, Russia, India and China – surpasses the cumulative GDP of the EU. And according to experts this gap will only increase in the future. There is no reason to doubt that the economic potential of the new centres of global economic growth will inevitably be converted into political influence and will strengthen multipolarity.[159]

The Asian macroregional context is enriched by the contributions of regional organizations other than the SCO. For instance, ASEAN members (Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and

---

[158] *Joint Statement 14th India-EU Summit*, ¶ 9, EUROPEAN COMMISSION (Oct. 6, 2017), europa.eu/rapid/press-release_STATEMENT-17-3743_en.htm.

[159] Vladimir Putin, President, Russian Federation, The Universal, Indivisible Character of Global Security (Feb. 11, 2007), *available at* https://www.globalresearch.ca/the_universal-indivisible-character-of-global-security/4741.

Vietnam) have been particularly active in information security over the last decade. In 2011, their ICT Masterplan included the development of a common framework for information security, to be preceded by a campaign to promote cyber security.[160] An enhanced attention paid to cybersecurity is traceable to the Masterplan elaborated four years later and announced through the Da Nang Declaration.[161] This renewed Masterplan "focuses on the increasing prospect of cyber threats—both economic and social—posed by malicious software, hacking, data theft and online fraud," and in so doing, shifts from a military conception of cyber security to one concerned with commercial implications of cyber espionage and intrusion.[162] Such a pivot was already clearly established in the completion report of the previous version of the Masterplan, stressing the need for standardization of digital transaction regulations across ASEAN countries in order to promote secure electronic authentication, identity proofing, and privacy protection.[163] In a declaration signed with Australia a few months ago, ASEAN expressed its commitment to countering transnational cybercrime by promoting a framework of

> international stability for cyberspace based on *existing international law*, cooperative capacity building, practical confidence building measures, *voluntary, and non-binding* norms of *responsible* behaviour taking reference from the 2015 Report of the UN Group of Governmental Experts on Developments in the Field of Information and

---

[160] *ASEAN ICT Masterplan 2015: We're Stronger When We're Connected*, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Jan. 13, 2011), https://www.asean.org/wp-content/uploads/images/2012/publications/ASEAN%20ICT%20Masterplan%20(AIM2015).pdf.

[161] *Da Nang Declaration: Towards a Digitally-Enabled, Inclusive, Secure and Sustainable ASEAN Community*, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Nov. 27, 2015), https://www.asean.org/wp-content/uploads/images/2015/November/statement/DA%20NANG%20DECLARATION.pdf.

[162] *ASEAN ICT Masterplan 2020*, 16, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Nov. 2015), *available at* https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ASEAN%20ICT%20masterplan%202020.pdf.

[163] *ASEAN ICT Masterplan 2015: Completion Report*, 76–77, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Dec. 2015), *available at* https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ASEAN%20ICT%20Completion%20Report.pdf.

> Telecommunications in the Context of International Security.[164]

Last April, a statement confirmed ASEAN's commitment to non-binding norms, although it added that "the promotion of cyber norms of responsible state behaviour is important for cultivating trust and confidence *and the eventual development of a rules-based cyberspace*."[165] This latter consideration arguably discloses the interest for possible binding norms in the near future at the regional and interregional level.[166] Moreover, the statement further strengthened ASEAN cooperation on personal data protection in cyberspace.[167] The most recent relevant ASEAN policy traces back to a couple of months ago, and confines itself to reiterating the organization's effort to counter cyber threats and incidents by facilitating information sharing, arranging emergency response teams, identifying *voluntary* norms of state behavior, improving

---

[164] *Joint Statement of the ASEAN-Australia Special Summit: The Sydney Declaration*, ¶¶ 11, 14, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Mar. 18, 2018), https://asean.org/wp-content/uploads/2018/03/Joint-Statement-of-the-ASEAN-Australia-Special-Summit-Sydney-Declaration-FINAL.pdf (emphases added). It is important to note the term "responsible" and to place it in the sliding scale of legal terminology which usually situates "responsibility" at one end, "duty" in the middle, and "obligation" at the other end.

[165] *ASEAN Leaders' Statement on Cybersecurity Cooperation*, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Apr. 27, 2018), https://asean.org/wp-content/uploads/2018/04/ASEAN-Leaders-Statement-on-Cybersecurity-Cooperation.pdf (emphasis added).

[166] Sydney noted: "Australia recognizes that the elaboration of how international law applies to States' use of cyberspace is a long-term task. *In the short term*, there is a need for practical measures to address and prevent problems between States in cyberspace that may result from misperception and that could lead, through miscalculation and escalation, to conflict. Regional security organizations are particularly well-placed to consider, develop and implement cyber confidence-building measures. Australia is leading work within the [ASEAN] Regional Forum to advance this important agenda, which, in view of varying capacity among members, should include capacity-building objectives." U.N. Secretary General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, U.N.Doc. A/69/112, at 3 (June 30, 2014) (emphasis added). For the counterterrorism context of ASEAN Regional Forum's cybersecurity engagement, see Takeshi Yuzawa, *The ASEAN Regional Forum: Challenges and Prospects*, *in* ROUTLEDGE HANDBOOK OF ASIAN REGIONALISM 338 (Mark Beeson & Richard Stubbs eds., 2012).

[167] *Chairman's Statement of the 32nd ASEAN Summit*, ¶ 6, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Apr. 28, 2018), https://asean.org/wp-content/uploads/2018/04/Chairmans-Statement-of-the-32nd-ASEAN-Summit.pdf.

technical digital literacy, and ensuring personal data protection.[168] Contrary to the "hard approach" of countries like Russia and China,[169] this policy also underlined the need to promote "principles such as peace, tolerance, respect for diversity and moderation as a counter-narrative" to prevent the misuse of cyber tools for terrorist activities and extremist propaganda.[170]

The Western block, as we may slightly improperly call it, is mainly based on the joint preferences and aspirations of the EU, the US, Canada, and Japan. There is evidence of Brussels' agreement with Washington that existing *hard* laws should be accompanied by new *soft* ones, especially applicable to wartime and peacetime respectively.[171] In other words, the EU affirms the centrality of the binding UN Charter for the governance of cyber activities, to be complemented by universal non-binding norms specifically designed on ICTs and based on responsible behaviors as well as confidence-building measures.[172]

> In this context, [the EU] emphasize[s] the following which, *inter alia*, apply to State use of ICTs: sovereign equality; non-intervention in the internal affairs of other States; the obligation to settle international disputes by peaceful means in such a manner that international peace, security, and justice are not endangered; the right to respond, including by non-forcible countermeasures, to internationally wrongful acts committed

---

[168] *Joint Communiqué of the 51st ASEAN Foreign Ministers' Meeting*, ¶¶ 12, 14, 15, 33, 48, 68, ASSOCIATION OF SOUTHEAST ASIAN NATIONS (Aug. 2, 2018), https://asean.org/wp-content/uploads/2018/08/51st-AMM-Joint-Communique-Final.pdf.

[169] And indeed, someone conceives a possible ASEAN-US "Code of Conduct" for the near future. *See, e.g.*, Lindsey W. Ford, *The U.S.-ASEAN Partnership in the Indo-Pacific*, ASIA SOC'Y POL'Y INST., at 9 (July 23, 2018), https://asiasociety.org/sites/default/files/2018-07/US-ASEAN%20Paper_2.pdf.

[170] *Joint Communiqué of the 51st ASEAN Foreign Ministers' Meeting*, *supra* note 168, ¶ 77.

[171] *Building an Effective European Cyber Shield: Taking EU Cooperation to the Next Level*, EUR. POL. STRATEGY CTR., at 14 (May 8, 2017), https://ec.europa.eu/epsc/sites/epsc/files/strategic_note_issue_24.pdf.

[172] *EU Statement – United Nations 1st Committee: Thematic Discussion on Other Disarmament Measures and International Security*, ¶ 4, EUROPEAN UNION EXTERNAL ACTION (Oct. 23, 2017), https://eeas.europa.eu/headquarters/headquarters-homepage/36640/eu-statement-%E2%80%93-united-nations-1st-committee-thematic-discussion-other-disarmament-measures-and_en.

> through the use of ICTs; the obligation to refrain in 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 purposes of the United Nations; respect for human rights and fundamental freedoms; the inherent right to self-defence; and international humanitarian law, including the principles of precaution, humanity, necessity, proportionality and distinction.[173]

The Group of Seven (G7), consisting of the most industrialized countries of the "Global North," subscribed to these words, specifying that not only the UN Charter, but also human rights customs and treaties, shall play a remarkable role in shaping cyber governance worldwide.[174] Interestingly, these governments also "call[ed] on States to publicly explain their views on how existing international law applies to States' activities in cyberspace to the greatest extent possible in order to improve transparency and give rise to more settled expectations of State behaviour."[175] Obviously, translating this slogan into facts and legislation is extremely arduous, and the preferred language for implementation tasks prioritizes awareness, coordination, knowledge sharing, and good practices.[176]

---

[173] *Id.* at ¶ 5.

[174] To this effect, the (re-)transformation of the G8 into the G7 has borne normative consequences of outstanding momentum. *See generally* Gordon S. Smith, *G7 to G8 to G20: Evolution in Global Governance*, CENTRE FOR INT'L GOVERNANCE INNOVATION (May 2011), https://www.cigionline.org/sites/default/files/g20no6-2.pdf. The President of the United States has recently called for the readmission of Russian Federation into the club, possibly to attempt coordination at curbing cyber-attacks which are damaging the US economy. *See* Julian Borger & Anne Perkins, *Donald Trump calls for G7 to readmit Russia ahead of summit*, THE GUARDIAN (June 9, 2018), https://www.theguardian.com/world/2018/jun/08/donald-trump-shows-no-sign-compromise-flies-in-g7-summit.

[175] *G7 Declaration on Responsible States Behaviour in Cyberspace*, G7 (Apr. 11, 2017), http://www.g7italy.it/sites/default/files/documents/Declaration_on_cyberspace.pdf.

[176] *G7 Actions for Enhancing Cybersecurity for Businesses*, G7 (Sept. 26, 2017), http://www.g7italy.it/sites/default/files/documents/ANNEX3-Actions_Cybersecurity_0.pdf. A noticeable step forward—but still fashioned in a non-binding, recommending language—is the most recent G7's Dinard Declaration on the Cyber Norm Initiative (6 April 2019), reiterating the

For instance, one may wonder how the non-intervention in states' domestic affairs could be reconciled with states' right to self-defense.[177] Unsurprisingly, these are longstanding issues discussed at the UN level over the last twenty years; this process signposted the milestones of the global dialogue on the matter, although substantial division on several key problems remains. Despite these difficulties, the United Nations offers a unique forum for the in-depth discussion and negotiation of the Eastern and Western stances.[178] For instance, while the views within the aforementioned G7 are quite consistent, the G20—which consists of Western countries, Russia, and developing powers like India and China—carefully avoids to engage in trade-offs on cyber security:

> Compared to traditional international organizations, the G20 resembles a loosely organized network or informal gathering. Meetings take place in different locations, there are no procedural rules and its output is anything but a treaty or any other form of traditional international law… [I]t can focus on activities such as agenda-setting, policy coordination, consensus-building and the distribution of tasks across existing institutions.[179]

A recent declaration touched upon digital trade-related policy areas, such as intellectual property rights, digital start-up innovation,

---

commitment to "promoting an open, secure, stable, accessible and peaceful cyberspace for all, where the application of international law and fundamental freedoms are promoted and human rights are protected online." Dinard Declaration on the Cyber Norm Initiative, G7 (Apr. 6, 2019), http://www.g7.utoronto.ca/foreign/190406-cyber.html.

[177] Since self-defence does not require prior UNSC authorization, it is not subject to direct or hidden vetoes. HIGGINS, *supra* note 77, at 227.

[178] Borrowing from the submission of the Russian representatives, "[t]he use of information and telecommunication technologies and methods is directly related to the establishment of military and political security in countries throughout the world, and it should therefore be considered in a global, comprehensive and non-discriminatory manner with the participation of as many countries as possible on the basis of the principle of equitable geographical distribution. Consideration of the issue under the auspices of the United Nations would provide just such an approach. As an important international organization which most fully represents the interests of all countries and plays a coordinating role in the area of disarmament, the United Nations provides a foundation for a balanced and effective system of global security," U.N. Secretary General, *Developments in the Field of Information and Telecommunications in the Context of International Security*, 9, U.N.Doc. A/58/373 (Sept. 17, 2003).

[179] Wouters & Geraets, *supra* note 43, at 20–22.

online privacy and electronic data protection, leaving traditional security aspects aside and refraining from commenting on which forum—besides the WTO—should take the lead in fostering consensus on cyber issues.[180] Similar considerations are valid for the OSCE, which encompasses countries under both the Atlantic block's and the Russian sphere of influence: This security organization headquartered in Vienna mainly addresses conflict prevention in cyberspace as well as confidence-building measures,[181] with no attempt at promoting itself as a policy-bargaining forum on sensitive details.[182]

At the sunrise of the 21st century, the United Nations General Assembly was already concerned with possible cyber-attacks on critical national infrastructures, and urged states to cooperate in tracing and investigating these attacks by sharing information on their alleged perpetrators; it equally encouraged every country to legislate on the matter, building a strong procedural and substantial legal framework to make those perpetrators accountable *domestically*.[183] The theoretical understanding today is that a number of key civilian infrastructures—like financial and civil aircraft systems—cannot be hacked by states under any circumstance, although the US still shows reluctance to accept this constraint.[184] Internationally, however, no mention was made to treaties on cyber security. In contrast, the second decade of this century is witnessing a fervent debate on the international instrument which would best serve the purpose of examining "*at multilateral levels* the consideration of existing and potential threats in the field of information security, as well as possible measures to limit the threats emerging in this field, *consistent with the need to preserve the free flow of information*."[185] Over the past several years, the General Assembly has repeatedly invited *all* the UN Members to

---

[180] *G20 Leaders' Declaration: Shaping an Interconnected World*, G20, at 5–6 (July 8, 2017), https://www.g20germany.de/Content/EN/_Anlagen/G20/G20-leaders-declaration___blob=publicationFile&v=11.pdf.

[181] *See, e.g.*, Organization for Security and Co-operation in Europe (OSCE), *OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies*, OSCE Doc. PC.DEC/1202 (Mar. 10, 2016), https://www.osce.org/pc/227281?download=true.

[182] Luigi Martino, *Give Diplomacy a Chance: OSCE's Red Lines in Cyberspace*, ITALIAN INST. FOR INT'L POL. STUD. (May 2, 2018), https://www.ispionline.it/en/pubblicazione/give-diplomacy-chance-osces-red-lines-cyberspace-20377.

[183] G.A. Res. 58/199, annex ¶¶ 7, 9, 10 (Jan. 30, 2004).

[184] BARRERA, *supra* note 101, at 7.

[185] G.A. Res. 64/25, ¶ 1 (Jan. 14, 2010) (emphases added).

overcome the United Nations Security Council (UNSC) impasse and share their official positions with regards to information security, so as to prepare its own negotiating agenda.[186] On a more positive note, it has recognized the risks inherent in unbalanced development strategies hindered by a digital divide, praising the growth that shared and fair connectivity and ICT governance may trigger in societies still left behind.[187] Four years ago, on the legal basis of a previous mandate,[188] the Assembly

> [w]elcome[d] the commencement of the work of the Group of Governmental Experts, and authorize[d] the Group […] to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, *including norms, rules or principles* of responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts *and how international law applies to the use of information and communications technologies* by States.[189]

The same task was reassigned to the Group of Governmental Experts (GGE) the following year.[190]

"*At the suggestion of the Russian Federation*, a GGE on the topic of information security was convened in 2004 [but t]he group failed to reach agreement."[191] The first consensual UN GGE report opted for vague language on the nature and prosecution of cybercrimes, but also considered "[n]on-criminal areas of transnational concern[, including] the risk of misperception resulting from a lack of shared understanding regarding international norms pertaining to State use of ICTs, which could affect crisis management in the event of major

---

[186] G.A. Res. 65/41, ¶ 3 (Jan. 11, 2011).
[187] G.A. Res. 65/141, ¶¶ 2, 4 (Feb. 2, 2011).
[188] G.A. Res. 66/24, ¶ 4 (Dec. 13, 2011).
[189] G.A. Res. 69/28, ¶ 4 (Dec. 11, 2014) (emphases added).
[190] G.A. Res. 70/237, ¶ 4 (Dec. 30, 2015).
[191] Ben Baseley-Walker, *Transparency and Confidence-building Measures in Cyberspace: Towards Norms of Behaviour*, 4 DISARMAMENT F.: CONFRONTING CYBERCONFLICT, at 37 (2011), *available at* https://citizenlab.ca/cybernorms2012/BaseleyWalker2011.pdf.

incidents."[192] The second report unfortunately keeps its rather descriptive approach, although it digs deeper into issues concerning the pure law. It notes the first version of the "Code of Conduct" introduced above, affirms that international law *is* applicable to cyber operations, and calls upon states for an intensification of legal harmonization, not secondarily on cooperation amongst law enforcement and prosecutorial agencies.[193] It further specifies that "States *must meet their international obligations regarding* internationally wrongful acts *attributable* to them. States *must not* use proxies to commit internationally wrongful acts. States *should seek to ensure that* their territories are not used by non-State actors for unlawful use of ICTs."[194] This sentence presents at least three open problems: the well-known drama of anonymity and attribution of cyber acts, the compromised language of "seeking to ensure," and the expression "unlawful use of ICTs."[195] Indeed, nobody can tell with full confidence what is unlawful in cyberspace, with a majority of scholars claiming that, for example, cyber espionage should *not* be deemed unlawful—and as such, lawful—in light of the *international* legal framework as it presently stands.[196] The report

---

[192] Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., ¶ 14, U.N. Doc. A/65/201 (July 30, 2010).

[193] *Id.* ¶¶ 19, 22.

[194] Rep. of the Grp. of Governmental Experts on Devs. in the Field of Info. and Telecomms. in the Context of Int'l Sec., ¶ 23, U.N. Doc. A/68/98 (June 24, 2013) (emphases added).

[195] A.A. Streltsov, *International Information Security: Description and Legal Aspects*, 3 DISARMAMENT F.: ICTS AND INT'L SEC., at 11 (2007), https://www.peacepalacelibrary.nl/ebooks/files/UNIDIR_pdf-art2642.pdf.

[196] International "state practice has recognized a right to clandestine intelligence collection as part of foreign relations policy. It is only unlawful under the domestic law of most states." Barmin et al., *supra* note 104, at 84; *see also* MANUEL, *supra* note 105, at 269. Despite this, diplomats engaged in acts of (cyber) espionage in their receiving countries may be declared *personae non gratae*. TOM OBOKATA, TRANSNATIONAL ORGANISED CRIME IN INTERNATIONAL LAW 73 (2010). In 2013, "representatives of States expressed concerns about the electronic espionage or the interception of information and data conducted by foreign States[, leading to] the UN General Assembly resolution on the *Right to Privacy in the Digital Age*." KITTICHAISAREE, *supra* note 83, at 8. The reason for this is that "because 'intelligence collection' is not a defined term, the absence of a per se prohibition on these activities does not settle the question of whether a specific intelligence collection activity might nonetheless violate a provision of international law. . . . In certain circumstances, one State's non-consensual cyber operation in another State's territory *could* violate international law, even if it falls below the threshold of a use of force." Brian J. Egan, *International Law and Stability in Cyberspace*, 35 BERKELEY J. INT'L L. 169, 174 (2017). This last stance is advocated by China, in the same vein as for other international policy

recommends to "build upon progress made bilaterally and multilaterally, including in regional groups" and to engage in "regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums, *and other international organizations*,"[197] in order to set up "regulatory frameworks to fulfil their responsibilities" (the choice of "responsibilities" in lieu of the more demanding "obligations" is worth noticing).[198] The third report's Chapter IV, titled "How international law applies to the use of ICTs," taking in due regard the second version of the SCO's proposed "Code of Conduct," tries to take a step forward in the definition of the legal duties of states in cyber matters. Much of the outcome is still principled in nature, even though a couple of points are worth mentioning: "the inherent right of States to take measures consistent with international law and as recognized in the Charter," and the balancing observation that "the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State[, hence] the accusations of organizing and implementing wrongful acts brought against States should be substantiated."[199] These wise considerations trigger the issue of how to prove the allegations or, in other words, what threshold of probability is acceptable as evidence—indeed, it is infamously known that absolute proof is very arduous to reach about cyber activities—an issue which requires further elaboration and may obstruct the process for a very long time. The outcome of the last negotiation round was not surprising at all:

---

domains: in general, one must exercise due caution in importing conclusions from other IL regimes; however, drawing a parallel with international law of the sea may hold some significance for the issue at stake here. "Opinions are . . . divided on the right to conduct intelligence-gathering activities . . . in the EEZ of another state without its consent. Even the very concept of the 'peaceful uses' or 'peaceful purposes' referred to in the [UNCLOS] is the subject of disagreement with China arguing that any activities by military vessels and aircraft are *ipso facto* not peaceful, while the United States argues that non-aggressive activities that do not involve *the threat or* use of force contrary to Article 2(4) of the United Nations Charter are fully permitted." Rosemary Rayfuse, *Some Reflections on What's Wrong with the Law of the Sea*, in WHAT'S WRONG WITH INTERNATIONAL LAW? 16, 21 (Cedric M.J. Ryngaert et al. eds., 2015) (second emphasis added).

[197] U.N. Doc. A/68/98, *supra* note 194, ¶¶ 27, 29.

[198] *Id.* at ¶ 30. The use of the word "responsibilities" in lieu of the more demanding "obligations" is worth noting.

[199] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, ¶ 28(c), (f), U.N. Doc. A/70/174 (July 22, 2015).

> [s]everal draft substantive reports were considered by the [UN GGE], on the following issues: existing and emerging threats; capacity-building; confidence-building; recommendations on the implementation of norms, rules and principles for the responsible behaviour of States; application of international law to the use of information and communications technologies; and conclusions and recommendations for future work. No consensus was reached on a final report.[200]

Such a breakdown was seen by many as the last say on the matter, but the urgency of the topic forced states back to the negotiating table once again.[201] Last October, two competing resolutions were presented at the UN, one sponsored by Russia—notably, no longer by the SCO—the other by the US.[202] The first established an Open-Ended Working Group (participated in by more countries) while the second called for another round of GGE.[203] Both have been adopted.[204] However, any excitement is misplaced: firstly, because the two resolutions were presented as mutually exclusive;[205] secondly, because the Paris Call for Trust and Security in Cyberspace launched last November at the UNESCO Internet

---

[200] U.N. Secretary-General, *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security*, ¶ 5, U.N. Doc. A/72/237 (Aug. 14, 2017).
[201] Stefan Soesanto & Fosca D'Incau, *The UN GGE is Dead: Time to Fall Forward*, EUR. COUNCIL FOREIGN REL. (Aug. 15, 2017), https://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; Alex Grigsby, *The End of Cyber Norms*, 59 SURVIVAL 109 (2017).
[202] Deborah Brown, *UN General Assembly adopts record number of resolutions on internet governance and policy: Mixed outcomes for human rights online*, ASSOCIATION FOR PROGRESSIVE COMMUNICATIONS (Jan. 10, 2019), https://www.apc.org/en/news/un-general-assembly-adopts-record-number-resolutions-internet-governance-and-policy-mixed.
[203] U.N., G.A. First Comm., Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/C.1/73/L.27/Rev.1 (Oct. 29, 2018); U.N., G.A. First Comm., Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, U.N. Doc. A/C.1/73/L.37 (Oct. 18, 2018).
[204] G.A. Res. 73/27 (Dec. 11, 2018).
[205] Alex Grigsby, *The United Nations Doubles Its Workload on Cyber Norms, and Not Everyone Is Pleased*, COUNCIL ON FOREIGN RELATIONS (Nov. 15, 2018), https://www.cfr.org/blog/united-nations-doubles-its-workload-cyber-norms-and-not-everyone-pleased.

Governance Forum (IGF) by the President of France has not gathered the support of either country.[206]

Given these discouraging circumstances, it seems impossible to predict when and on what grounds any consensus between the two blocks—if we may still call "the East" and "the West" that way—will be officially resumed.[207] It appears wise to resort to the expertise of the International Law Commission (ILC) whose non-binding findings, related to the codification of customs and the progressive development of public international law, are nevertheless expressions of authoritative scholarship, and as such are highly regarded by governments and judicial bodies (including the International Court of Justice).[208] The ILC, although still residually targeted with criticisms of pro-West bias, might be able to find acceptable legal adjustments by building on its Draft Articles on Responsibility of International Organizations (2011) and Draft Articles on the Responsibility of States for Internationally Wrongful Acts (2001), pondering the suggestions made in the second edition (2017) of the Tallinn Manual (the "Manual"), whilst accommodating some of the quests coming from the SCO and other non-Western institutional arrangements.[209] In this way, it may overcome the impasse at the UNGA as well as the hidden vetoes deadlocking the Security Council.[210] Regrettably, as informally noted by the ILC itself, the *Manual*'s acceptance is often overpriced: among the

---

[206] China, Russia and the US did not sign the Call, which is an eloquent choice, considering that it is not even a binding document and received strong endorsement from the private sectors of all these countries. *See Cybersecurity: Paris Call of 12 November 2018 for Trust and Security in Cyberspace*, FRENCH DIPLOMATIE (Nov. 12, 2018), https://www.diplomatie.gouv.fr/en/french-foreign-policy/digital-diplomacy/france-and-cyber-security/article/cybersecurity-paris-call-of-12-november-2018-for-trust-and-security-in.

[207] Alex Grigsby, *Unpacking The Competing Russian and U.S. Cyberspace Resolutions at the United Nations*, COUNCIL ON FOREIGN RELATIONS (Oct. 29, 2018), https://www.cfr.org/blog/unpacking-competing-russian-and-us-cyberspace-resolutions-united-nations.

[208] François Delerue, *The Codification of the International Law Applicable to Cyber Operations: A Matter for the ILC?*, ESIL REFLECTIONS (July 3, 2018), http://esil-sedi.eu/wp-content/uploads/2018/06/ESIL-Reflection-Delerue.pdf.

[209] KITTICHAISAREE, *supra* note 83, at 43.

[210] The ILC is more effective in codification than in progressive development. Rosanne van Abeleek, *The Proliferation of Law-making Organs: A New Role for the International Law Commission?*, *in* PROLIFERATION OF INTERNATIONAL ORGANIZATIONS: LEGAL ISSUES 219, 224 (Niels M. Blokker & Henry G. Schermers eds., 2001). A cyberlaw report issued by the Commission would probably favor those States which advocate for an application of current public international law regimes to the cyberspace, as opposed to the creation of new, cyberspace-tailored rules.

"cyber powers," even the UK seems to reject its systematization bid, whilst the US notoriously prefers to keep a high degree of indeterminacy on the international legal framework applicable to cyber operations.[211] Coupled with the last UN GGE's failure just mentioned, this cold-hearted endorsement of the *Manual* testifies once more to the compelling importance of looking at what preferences non-Western regional organizations like the SCO are trying to negotiate internally and uphold before the international community. In the words of its general editor, the *Manual*—the drafting thereof being also participated by a few Eastern leading scholars like Professor HUANG Zhixiong from Wuhan University Law School (who was also, notably, educated in Mainland China, including for his PhD)—had no prescriptive function to play; it was rather intended as an interpretative device for states to make informed decisions in light of the possible interpretations to be attached to the "state of the art" in international law.[212] Even though, as stated above, the *Manual*'s acceptance is overestimated, its normative influence should not go underrated: "[I]nstitutionalization may follow, rather than precede, the initiation of a norm cascade," and the *Manual* stands as a prominent candidate for such an initiation.[213] Stripped of beyond-NATO institutional endorsements and left in the hands of mainstreamed Western scholars, the *Manual 2.0* is little more than a private enterprise, and yet, "privately written legal treatises might influence behavior by clarifying custom."[214]

Whether cyber-attacks of sufficient scale may justify conventional military countermeasures is an issue which needs to be solved legally by an organ generally perceived as *super partes*, as diplomacy has repeatedly failed to reach a compromise. An ILC

---

[211] Int'l Law Comm'n, 67th Sess., 3265th mtg. at 9, U.N. Doc. A/CN.4/SR.3265 (Aug. 7, 2015); Dan Efrony & Yuval Shany, *A Rule Book on the Shelf? Tallinn Manual 2.0 on Cyberoperations and Subsequent State Practice*, 112 AM. J. INT'L L. 583, 585 (2018). One may compare this attitude with the US endorsement of other non-UN codifications of and commentaries upon international humanitarian law customs, for example the ICRC's "Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law." Steven R. Ratner, *Sources of International Humanitarian Law and International Criminal Law: War/Crimes and the Limits of the Doctrine of Sources*, *in* THE OXFORD HANDBOOK ON THE SOURCES OF INTERNATIONAL LAW 912, 919 (Samantha Besson & Jean d'Aspremont eds., 2017).

[212] Michael N. Schmitt, *International Cyber Norms: Reflections on the Path Ahead*, at 5 (2018), *available at* https://ore.exeter.ac.uk/repository/handle/10871/33829.

[213] Finnemore & Sikkink, *supra* note 29, at 900.

[214] RICHARD H. MCADAMS, THE EXPRESSIVE POWERS OF LAW: THEORIES AND LIMITS 115 (2015).

report or an International Court of Justice advisory opinion would not necessarily settle practical behaviors. Nevertheless, they would represent a first authoritative step forward. Meanwhile, India "has kicked off a process that will pick up the pieces from a set of decade-old United Nations cyber-warfare negotiations."[215] This process' first findings seem to see "in the country's best interest to acknowledge an express affirmation of a right to self-defense, giving way, as it would, for an option to respond to potential Pakistani or Chinese cyber hostilities through conventional means."[216] The fact that both Pakistan and China are SCO members speaks volumes of the hurdles any SCO-negotiated compromise on cybersecurity would need to overcome: before turning any common stance into Codes like the two brought before the attention of the international community when the SCO was led by Moscow and Beijing, it would need to embed New Delhi in the "Eastern" normative discourse.

VII. THE CENTRALITY OF LANGUAGE

> To external observers, dialogue between Russia and Western partners on cyberspace issues seems characterised by mutual incomprehension and apparent intransigence. Norms which are taken for granted on one side are seen as threatening by the other, and the lack of a common *vocabulary* or common *concepts* relating to cyberspace means that even when attempts are made to find common ground, these attempts soon founder.[217]

The analysis above has tangentially touched upon a rather fundamental issue: the linguistic one, which will be focused on in this last section. Written law is obviously made of linguistic

---

[215] Anuj Srivas, *After UN Talks on Cyber Norms Collapse, India Starts Chalking Out Own Strategy*, THE WIRE (Sept. 12, 2017), https://thewire.in/tech/un-cyber-norms-india-asoke-mukerji-nsc.
[216] *Id.*
[217] GILES, *supra* note 92, at 64 (emphases added).

(non-)choices, and the very same document may read substantially differently when translated into various languages. This occurs in the first place at the UN level, where six official languages are used; the case of the ICCPR is emblematic: "the English and revised draft of ICCPR Article 4(1) both say that rights may only be derogated when doing so is 'strictly' required by an emergency, whereas the Covenant in Chinese says it must be 絕對 (absolutely) required. (The Russian version mistakenly says only 'required,' without adding either adverb)."[218] And this is not all: unofficial Chinese versions of the ICCPR have circulated for decades under the tacit consent of diplomatic and political establishments, and to one's dismay, although they contain clear discrepancies with the official text, they are regularly and confidently "quoted" by Chinese and non-Chinese scholars alike.[219]

Beyond this, most issues with language come with its consciously-resorted-to indeterminacy, which allows states and other entities to rely on unsettled linguistic vagueness in order to satisfy political appetites. "One of the primary issues with cybersecurity today . . . is the lack of agreement about definitions, which inhibits both lawmakers and military actors" and unleashes investments in cyber-weapons whilst blurring states' political accountability.[220] "[E]ven agreements that are seen as successful in the 'cyber' realm such as the 'US-China cyber agreement' leave much open to interpretation because of the language used," in the double perspective of language *as legal(istic) idiom* and language *as culturally-embedded conceptual vi*ew *on reality*.[221] English, today's imperialistic language, entertains a controversial relationship with cyber policymaking and lawmaking: on the one hand, less than thirty percent of Internet users master English as their mother or quasi-mother tongue, and this figure is destined to drop drastically due to the demographic trend and technology penetration in the "Global South" despite the upsurge in Indian users.[222] On the other hand,

---

[218] James D. Seymour & Patrick Yuk-Tung Wong, *China and the International Human Rights Covenants*, 47 CRITICAL ASIAN STUD. 514, 517 (2015).
[219] *Cf.* Shiyan Sun, *The Problems of the Chinese Texts of the International Human Rights Covenants: A Revisit*, 15 CHINESE J. INT'L L. 773 (2016).
[220] Barmin et al., *supra* note 104, at 91; *see also* Chaditsa Poulatova, *Cyber Threat vs Cyber Defence: Problems and Lessons Learnt*, at 345 (2017), *available at* http://www.iiis.org/CDs2017/CD2017Spring/papers/ZA275NG.pdf.
[221] Futter, *supra* note 11, at 209. Indeed, there is a "tendency to confuse the language of legal and social norms in discussions around cybersecurity and governance." McKune & Ahmed, *supra* note 14, at 3847.
[222] Choucri & Goldsmith, *supra* note 19, at 76.

English remains the top negotiating language internationally,[223] provides the original vocabulary for most technological tools,[224] and dominates the Internet through the Anglo-Saxon (model) corporations, platforms, software, and search engines.[225] It shares with German, French and other Western legal languages a common root in Latin as the former *lingua franca* of the European *ius commune*.[226] Most innovations nowadays are "born" in English, and their regulation cannot avoid undergoing a process of "translation" from English cultural and linguistic codes and business etiquettes.[227] *De facto*, the discrepancy between the Internet userbase and its formal or factual establishment, not secondarily in diplomatic and legal standard-setting procedures, is widening. The case of China is emblematic: hundreds of millions of Internet users utilize the web in Chinese exclusively, and yet, China negotiates cyber policies in English (formally in several fora, and informally at times even

---

[223] EVANGELOS RAFTOPOULOS, INTERNATIONAL NEGOTIATION: A PROCESS OF RELATIONAL GOVERNANCE FOR INTERNATIONAL COMMON INTEREST 49, 106 n.27, 146–148, 231 (2019); Jacqueline Mowbray, *The future of international law: Shaped by English*, VÖLKERRECHTSBLOG (June 18, 2014), https://voelkerrechtsblog.org/the-future-of-international-law-shaped-by-english/.

[224] Robert Henry Lawrence Phillipson, *The Linguistic Imperialism of Neoliberal Empire*, 5 CRITICAL INQUIRY IN LANGUAGE STUD. 1 (2008); Yukio Tsuda (津田幸男), *Critical Studies on the Dominance of English and the Implications for International Communication*, 10 JAPAN REV. 219, 234 (1998).

[225] Emma CHARLTON, *The internet has a language diversity problem*, WORLD ECONOMIC FORUM (Dec. 13, 2018), https://www.weforum.org/agenda/2018/12/chart-of-the-day-the-internet-has-a-language-diversity-problem/. For helpful infographics, see *Top Languages of the Internet, Today and Tomorrow*, UNBABEL BLOG (June 10, 2015), https://unbabel.com/blog/top-languages-of-the-internet/.

[226] Caroline I. B. Laske, *Translators and Legal Comparatists as Objective Mediators Between Cultures?*, *in* OBJECTIVITY IN LAW AND LEGAL REASONING 219 (Jaakko Husa & Mark Van Hoecke eds., 2013). *See also* Gleider Ignacio Hernández, *On Multilingualism and the International Legal Process*, at 6 (2010), *available at* http://dro.dur.ac.uk/8296/ ("The language of diplomacy had shifted earlier than the language of treaties, which until the eighteenth century remained—with some exceptions—Latin, when French became ascendant. This was an important shift for international law, from the use of a language which enjoyed no connection with a contemporary society towards a [*langue vivante*] attached to a contemporary society.").

[227] *Cf.* Fernando Prieto Ramos, *International and Supranational Law in Translation: From Multilingual Lawmaking to Adjudication*, 20 THE TRANSLATOR 313, 318 (2014) (arguing that the "process of cultural detachment or "deculturalization" is coupled with one of appropriation by the international community. English is used by drafters with many different backgrounds and mother languages. This reinforces the reduction of linguistic idiomaticity and enhances the "permeability" of English to non-idiomatic uses, including some "oddities" or "interferences in vocabulary and syntax").

within the SCO, notably after India joined the club).[228] This unbalance creates otherwise avoidable frictions and misunderstandings. For instance, the "security-for-one-is-security-for-all" doctrine—more formally referable to as "indivisibility of security"[229] —seems to stand well before both sides, while concealing profound disagreement

> simply because this common phrase has entirely different meanings in Russian and in English. Despite recognition and patient explanation that use of the identical phrase to refer to widely differing concepts leads to . . . frustration, the phrase continues to occur in both Western and Russian discourse leading to each side embarking on their own separate conversation.[230]

Quite the same happens with the expression "information warfare."[231] A Russian officer notably observed that at the UN level, despite the translation service, negotiators speak different languages and employ an apparently shared terminological portfolio while conceptually pursuing their own discursive agenda and normative vocabulary.[232]

"Beyond its normative function, international law is a tool for communication, offering linguistic elements aimed . . . at the coordinated formation *and transformation* of international rules."[233] The best depiction of the centrality of linguistic choices, paradoxes, definitions, and dominations belongs to the infamously blurred indeterminacy of (cyber)terrorism, and related "counter-terrorism"

---

[228] Based on personal knowledge that the author acquired from Ms. Olesya Dovgalyuk, "Yenching Scholar" at the Yenching Academy of Peking University (Beijing).

[229] "Indivisible security mean[s] that the security of each state of our region is inextricably linked with the security of every other state. Another way of putting this would be: Co-operation is beneficial to all participating States, while the insecurity in or of one participating State can affect the well-being of all." Secretary General Marc Perrin de Brichambaut, *The Indivisibility of Euro-Atlantic Security*, OSCE 18TH PARTNERSHIP FOR PEACE RESEARCH SEMINAR (2010). *See also* THE INDIVISIBILITY OF SECURITY: RUSSIA AND EURO-ATLANTIC SECURITY (Andrew Monaghan ed., NATO Defence College 2010).

[230] GILES, *supra* note 92, at 65.

[231] *Id.* at 68.

[232] ENEKEN TIKK-RINGAS, DEVELOPMENTS IN THE FIELD OF INFORMATION AND TELECOMMUNICATION IN THE CONTEXT OF INTERNATIONAL SECURITY: WORK OF THE UN FIRST COMMITTEE 1998–2012 7 (2012).

[233] ATTILA MASSIMILIANO ENRICO TANZI, INTRODUZIONE AL DIRITTO INTERNAZIONALE CONTEMPORANEO 4 (4th ed., 2013) (emphasis added).

activities.[234] Paradoxically, the more adjectives/adverbs are added to a noun/verb, and the higher the number of translations of that word, the more meanings are multiplied, and scopes become more undefined. More broadly, from the perspective of international law, there is no agreed definition of "terrorism" either.[235] In such matters, language—as the means through which law is conceived, codified, enforced, and even resisted—is a factor of primary importance, particularly so when the field is relatively embryonic, as is the case in cyber security. The original, and the other authoritative, versions of an agreement shape not only the definitions of key-terms, but most significantly, the culturally-embedded meaning(s) to be attributed to such expressions against a defined context. Similar to other terms but to a greater extent, terrorism is difficult to define legally because it is constantly evolving, politically shaped by the concept of fear, which is subjective and therefore hard to address by law, and built on the perception of what is "self" and "other" in the social discourse. Some authors are pessimistic enough to argue that post-structuralist observations can sustain a convincement that "there has been no comprehensive definition of terrorism and [there is] no hope for it in the near future."[236] This is disastrous, given the centrality terrorism endures in both Western and Eastern public policy narratives. Both Russia and China list terrorism among the so-called "Three Evils", together with separatism and extremism.[237]

---

[234] Marina Kaljurand, *United Nations Group of Governmental Experts: The Estonian Perspective*, *in* INTERNATIONAL CYBER NORMS: LEGAL, POLICY & INDUSTRY PERSPECTIVES 111 (Anna-Maria Osula & Henry Roigas eds., 2016), *available at* https://ccdcoe.org/uploads/2018/10/InternationalCyberNorms_Ch6.pdf.

[235] For the classical scholarly monograph on this definitory subject, see BEN SAUL, DEFINING TERRORISM IN INTERNATIONAL LAW (2008). *See also* HELEN DUFFY, THE "WAR ON TERROR" AND THE FRAMEWORK OF INTERNATIONAL LAW 17–46 (2015). Moreover, the United Nations General Assembly has recently expressed regret at the lack of a shared definition of "terrorism" internationally. Press Release, General Assembly, Fight against International Terrorism Impeded by Stalemate on Comprehensive Convention, Sixth Committee Hears as Seventy-Third Session Begins, GA/L/3566 (Oct. 3 2018), *available at* https://www.un.org/press/en/2018/gal3566.doc.htm.

[236] Seyyed Javad Emamjomezadeh et al., *A Post Structural Approach to Terrorism Crisis of Meaning*, 4 INT'L J. ECON., MGMT. & SOC. SCI. 151, 155 (2015); *cf.* Charlotte Heath-Kelly, *Post-Structuralism and Constructivism*, *in* ROUTLEDGE HANDBOOK OF CRITICAL TERRORISM STUDIES 63 (Richard Jackson ed., 2016).

[237] Alexander Cooley, *Russia and the Recent Evolution of the SCO: Issues and Challenges for U.S. Policy*, *in* THE POLICY WORLD MEETS ACADEMIA: DESIGNING U.S. POLICY TOWARD RUSSIA 8, 11 (Timothy J. Colton et al. eds. 2010). *See also* McKune & Ahmed, *supra* note 14, at 3841; Olcott, *supra* note 126, at 268 (stating that "the [Collective Security Treaty Organization] and SCO

Interestingly, with regards to linguistic shades of the term "terrorism", it has been noticed that "notwithstanding the lack of direct regulation of c*yber terrorism*, some cyber-attacks are still likely to fall within the scope of the wide general definitions of *terrorist offences* in some regional instruments[, including] the Shanghai Cooperation Organisation Convention on Combating Terrorism, Separatism and Extremism of 2001."[238] This lack of clarity in international legal practice on cyber terrorism, evidenced by the words like "some", "likely to", and "general," is mirrored by the underdeveloped state of public international legal theory on cyber terrorism.

If lexical choices in "capturing" normative values—and drafting policies accordingly—vary widely depending on the specific cultural environment underpinning a language, this has not prevented international law from becoming a shared discipline, and legal discourses from receiving contributions by countries with different linguistic backgrounds. Through structuralist lenses, this is because legal arguments retain a self-construed "grammar," an inner "texture," which is distinctive, and thus allows for a separation between the "legal" and the "political" ultimately defending the autonomy of the law.[239] While policies are largely codified, norms can implicitly shape behaviors. In the logic of international law, such behaviors are for instance mirrored in customary rules. Beijing's interest in international customary law is manifested by its role in the Working Group on Customary International Law under the Asian-African Legal Consultative Organization, whose cyber agenda has been enacted by a Chinese proposal.[240] Rather than engaging seriously in treaty-making, a country may participate in the multi-player game of discerning and codification of competing (claimed) customs;[241] in this way, deeply shaping "the law"

---

share many of the same goals, but the CSTO promotes real integration of the militaries of the [M]ember [S]tates while the SCO styles itself as an organization that understands modern security risks: secession, extremism, and terrorism").

[238] Ben Saul & Kathleen Heath, *Cyber Terrorism*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 147, 163 (Nicholas Tsagourias & Russell J. Buchan eds. 2015) (emphases added).

[239] Justin Desautels-Stein, *International Legal Structuralism: A Primer*, 8 INT'L THEORY 201, 205 (2016).

[240] Ma Xinmin, *Key Issues and Future Development of International Cyberspace Law*, 2 CHINA Q. INT'L STRATEGIC STUD. 119, 123 (2016).

[241] To put it differently, the identification of customs and their codification is preferred to the drafting of ex-novo treaty-based provisions. The substantive *legal* results may eventually coincide, whilst the procedural transaction costs and "*political* capital" invested in and spent for the two activities might differ remarkably.

(international legal order) instead of "the laws" (particularistic legal regimes) on the surface. Since cyber norms belong to newly-developed fields of law, the formation of international customs—especially when facilitated by the "harvesting catalysis" of international organizations—can be assessed against lower standards of consistency and time.[242] The always disputed[243]—but still authoritative—*opinio iuris* employs a psychological element which may be fruitfully investigated through the post-structuralist problematic "suspicion of subjectivity and of authorial intentionality" [244] derived from its "focus on individuality and difference [which] is not easily imported into international legal scholarship."[245] Post-structuralism may provide useful views on the way "suspicion of subjectivity" and "focus on individuality" can come together, given that "Derrida's most enduring philosophical legacy today . . . is the theory that all binary oppositions are essentially unstable," exactly like customs.[246] Since "the very way in which we construct the social world is textual [and] interpreting the world reflects the concepts and structures of language," in order to explore the possible meanings of the text, one must appreciate its possible practical applications in the real world.[247] There is neither

---

[242] South West Africa (Ethiopia v. South Africa), Judgment, 1966 I.C.J. 6, at 250–324 (July 18) (dissenting opinion of Tanaka, K.), *available at* https://www.icj-cij.org/files/case-related/46/046-19660718-JUD-01-06-EN.pdf.

[243] Somek, *supra* note 38, at 754 ("One can profess belief in custom as source of law only by glossing over the fact that it remains profoundly unclear how much usage by whom is necessary to constitute sufficient practice and what it takes to encounter *genuine opinio iuris*. It is unlikely that any theory of customary law would ever be capable of arriving at a satisfactory answer to this question. The reason for being pessimistic is that convincing accounts would invariably have to move custom into a direction where it would appear increasingly similar to a process of legislation, for example, by specifying the number of confirmations, valid modes of expressing consent and constitutional principles that it is required to respect.").

[244] John R. Morss, *Structuralism and Interpretation in the Theory of International Law: Cracking the Code?*, at 6 (May 18, 2016), *available at* https://ssrn.com/abstract=2781388.

[245] Christopher M.J. Boyd, Examining (International) Law: Towards a Systematic, Coherent and Radical Theory (April 26, 2012) (unpublished LL.M(R) thesis, University of Glasgow), http://theses.gla.ac.uk/3312/.

[246] Akbar Rasulov, *International Law and the Poststructuralist Challenge*, 19 LEIDEN J. INT'L L. 799, 800 (2006); *see also* Juliana Neuenschwander Magalhães & José Antonio Rego Magalhães, *Law, Institutions, and Interpretation in Jacques Derrida*, 13 DIREITO GV L. REV. 586, 593 (2017).

[247] Steven Murray Smith & Patricia Owens, *Alternative Approaches to International Theory*, *in* THE GLOBALIZATION OF WORLD POLITICS: AN INTRODUCTION TO INTERNATIONAL RELATIONS 287 (Steven Murray Smith & John Baylis eds., 3d ed., Oxford Univ. Press 2005).

definitive reading of a legal text nor authority, but only competing readings representing competing patterns of aspiring dominations. It follows that the alternative implications of the textual structures of a treaty cannot be analyzed prior to witnessing the various interpretations given to them by actual political actors. These considerations trigger new relationships between treaty-based and custom-based norms of international law, and create opportunities for new actors to shape the international law discourse. The US publicly advocates for a free cyberspace, as its identity is naturally versed to preserve the power projection linked to a US-dominated cosmopolitanism,[248] whereas competing great powers like Russia and China instead prefer "boundaries in cyberspace, [which] are theorized to be an ontological necessity in order to preserve state identity."[249] This anthropological necessity is transferred into the customarization of social practice, and eventually into preferences of policymaking strategy.

NGOs have criticized the SCO's definition of terrorist activities as exaggeratedly far-reaching.[250] By joining the SCO and bringing English into it, India subscribed to the Organization's old "reciprocal recognition of a terrorist, separatist, or extremist act regardless of whether the legislation of SCO [M]ember [S]tates includes a corresponding act in the same category of crimes *or whether the act is described using the very same terms*," which arguably extends to cyberterrorism as well.[251] However, Indian *practical* understanding may differ. In India, "new thinking on international law borrows from the post-colonial deconstructionist methodologies," not to remain trapped in the "experience of disenchantment with an Enlightenment-induced modernity" which was the true essence of

---

[248] Maximilian Benedikt Mayer, The Unbearable Lightness of International Relations: Technological Innovations, Creative Destruction and Assemblages (2017) (unpublished Ph.D. dissertation, University of Bonn), http://hss.ulb.uni-bonn.de/2017/4652/4652.htm.

[249] Hans Jozef Adriaan Marie Simons, Consensual Hallucinations: The Politics of Identity in Dutch Cyber Security Policy, at 6 (July 2014) (unpublished M.Sc. thesis, Radboud University Nijmegen), https://theses.ubn.ru.nl/bitstream/handle/123456789/1121/Simons%2c_Hans_1.pdf?sequence=1.

[250] Linda Maduz, *Flexibility by Design: The Shanghai Cooperation Organisation and the Future of Eurasian Cooperation*, CTR. FOR SEC. STUD. (May 2018), http://www.css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Maduz-080618-ShanghaiCooperation.pdf.

[251] Council of Heads of SCO Member States Res. 1, *Concept of Cooperation Between SCO Member States in Combating Terrorism, Separatism, and Extremism*, art. 2, ¶ 3 (June 5, 2005) (emphasis added).

European colonialism.[252] In this sense, postmodern theories may better catch the sense of Indian choices with reference to the development of new international norms, by privileging the "discursive" and the "textual"[253] over the grounding of "the foundational concept of sovereignty upon a hierarchy of 'objective' social criteria (Civilisation; Development; Democracy)"[254] and, in so doing, disrupting binary dialectics[255] such as those between "securitization" and "democratization," "autochthonous" and "allogeneic" terrorist menaces,[256] "rational" and "irrational" social agents,[257] or "the East" and "the West."[258] This intent is achieved by capturing the influence of transplanted legal notions on patterns of domination and normative productions (*a fortiori* important regarding fields yet to be fully developed), and by deconstructing pretended-globalized explicit arguments in order to reach their "deep structure."[259] This is exercised through the separation of formal expressions and semiotic meanings, and the latter's detachment from the political and linguistic agency of the West's neo-imperialism (as much as from the paradigms retrievable in the variety of reactions to

---

[252] Prabhakar Singh, *Indian International Law: From a Colonized Apologist to a Subaltern Protagonist*, 23 LEIDEN J. INT'L L. 79, 88 (2010).

[253] Lene Hansen, *Poststructuralism*, *in* THE GLOBALIZATION OF WORLD POLITICS: AN INTRODUCTION TO INTERNATIONAL RELATIONS 287 (John Baylis et al. eds., 7th ed., Oxford Univ. Press 2017).

[254] ERIC WILSON, SAVAGE REPUBLIC: DE INDIS OF HUGO GROTIUS, REPUBLICANISM AND DUTCH HEGEMONY WITHIN THE EARLY MODERN WORLD-SYSTEM (C. 1600–1619) 59 (Martinus Nijhoff Publishers 2018).

[255] John Anthony Carty, *International Legal Personality and the End of the Subject: Natural Law and Phenomenological Responses to New Approaches to International Law*, 6 MELB. J. INT'L L. 534, 546–48 (2005).

[256] Morten Bay, *What is Cybersecurity? In Search of an Encompassing Definition for the Post-Snowden Era*, FRENCH J. FOR MEDIA RES., ¶ 42 (June 2016).

[257] Lene Hansen, *Poststructuralism and Security*, OXFORD RESEARCH ENCYCLOPEDIA INTERNATIONAL STUDIES, at 15 (Mar. 2010), http://internationalstudies.oxfordre.com/view/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-278?print=pdf ("The construction of 'terrorists' as 'irrational' intersected with poststructuralist deconstructions of rational-irrational dichotomies that had also been central to Cold War discourse. There was a call for theorizing the importance of emotion, passion, and feelings, not because these should be juxtaposed or privileged over 'rationality', nor because 'terrorists' should be redefined as 'rational', but because rationality assumptions were employed in security discourses with crucial implications for the identities that were constituted.").

[258] *Id.* at 9.

[259] Jean D'Aspremont, *Martti Koskenniemi, From Apology to Utopia: The Structure of International Legal Argument*, 19 REV. QUEBECOISE DE DROIT INT'L 353, 360 (2006).

the latter).[260] Indeed, "the *sense* of words such as 'law' and 'State' in European [and other] cultures differs to the extent that even the possibility of mutual understanding *seems* excluded."[261] In truth, the imperishable "deferment of meaning" so diligently described by Derrida helps shed a light upon the apparently interminable "deferment of compliant behavior" states should implement vis-à-vis one another in the cyber dimension (provided such a dimension exists and can be actually defined).[262]

VIII. CONCLUDING REMARKS

> Every choice is contingent upon what is presumed to be knowledge. To live without an awareness of the requirements of intelligent artisanship can leave a community as ravaged as if it had survived the destruction of warfare.[263]

Today's *(non-)*international law is traversed by entirely unprecedented tensions of dominance and patterns of disruption.[264] Against this backdrop, the risk of shaping the legal governance of cyber matters in a way close to the "model" represented by the intricate tangle of bilateral investment agreements—stripped of

---

[260] Nancy Armstrong & Leonard Tennenhouse, *History, Poststructuralism, and the Question of Narrative*, 1 NARRATIVE 45, 46, 49, 51 (1993); Wen-song Hwu, Toward Understanding Post-Structuralism and Curriculum 11, 20, 31 (May 1993) (unpublished Ph.D. dissertation No. 5516, Louisiana State University) (on file with LSU Digital Commons), *available at* https://digitalcommons.lsu.edu/gradschool_disstheses/5516; Margaret Jane Rabin & Frank Isaac Michelman, *Pragmatist and Poststructuralist Critical Legal Practice*, 139 U. PA. L. REV. 1019, 1037 n.73 (1991).

[261] *Id.* at 61 (emphases added). *See also* CATHERINE M. KELLOGG, LAW'S TRACE: FROM HEGEL TO DERRIDA 70 (Routledge 2009).

[262] I would prefer this translation over the more commonly used "deferral," as it incapsulates the idea of multiple partitions in addition to those of referral and time postponement/delay. It also suits actions—beyond terms—best.

[263] VINCENT OSTROM, THE QUEST TO UNDERSTAND HUMAN AFFAIRS: ESSAYS ON COLLECTIVE, CONSTITUTIONAL, AND EPISTEMIC CHOICE 267 (Barbara Allen ed., Lexington Books 2012).

[264] Is International Law International?, U.N. AUDIOVISUAL LIBRARY OF INTERNATIONAL LAW (Sept. 19, 2018), http://legal.un.org/avl/ls/AntheaR_IL_video_1.html.

coordinated coherence—is just around the corner.[265] This paper has fundamentally explained that three major stances are currently shaping global cyber governance: states that are satisfied with the legal *status quo*; those that seek to negotiate a binding treaty; and those that strive for the application of current hard laws on the one hand, and the negotiation of universal soft standards on the other.[266] This third group is the most numerous, although there is no agreement—neither in practice, nor in legal scholarship—on *how* to apply existing frameworks such as international humanitarian law, international human rights law, and international security law, made complex by the observation that "while a cyber 'weapon' may destroy civilian as well as military targets, it generally does not have kinetic impacts."[267]

Addressing the Internet's polycentric and multi-layered regulatory framework,[268] interesting and detailed proposals both *de lege lata* and *de lege ferenda* have been put forward by international publicists,[269] to pave the way ahead and try to recompose the fragmentation occurring within the SCO as well as the mistrust permeating the international attempts at finding common solutions based on minimum-denominator shared values. In the composite non-Western framework, India may make the most of its hybrid geopolitical identification in order to shape the international legal framework applicable to speculated-about threats and actual attacks in cyberspace. It has been argued that poststructuralist thinkers are well placed to shed light on how and *why* this may happen. In conclusion, *soft and hard* law, as much as *existing and new* norms,

---

[265] *See, e.g.*, Leilah Elmokadem, *Mapping of India's Cyber Security-Related Bilateral Agreements*, BANGALORE: CENTRE FOR INTERNET AND SOCIETY (2016) (highlighting the number and diversity of bilateral agreements signed by India on cybersecurity).

[266] MASSIMO DURANTE, ETHICS, LAW AND THE POLITICS OF INFORMATION: A GUIDE TO THE PHILOSOPHY OF LUCIANO FLORIDI 122–23 (Springer 2017) ("When technological scenarios and/or social customs change, the lawyer is called upon to consider whether the existing body of law has (at least potentially) foreseen this evolution; if so, the existing law can be interpreted extensively, thus maintaining some sort of continuity with the past . . . However, when a technological evolution involves a fracture . . . with the previous technology, the law is hard-pressed to adapt its existing categories to the changed technological reality.").

[267] KITTICHAISAREE, *supra* note 83, at 15.

[268] DURANTE, *supra* note 266, at 190.

[269] *See, e.g.*, Oona A. Hathaway et al., *The Law of Cyber-Attack*, 100 CALIF. L. REV. 817, 885 (2012); Kristen E. Eichensehr, *Cyberwar and International Law Step Zero*, 50 TEX. INT'L L.J. 355, 378 (2015); Wolff Heintschel von Heinegg, *International Law and International Information Security: A Response to Krutskikh and Streltsov*, 9 THE TALLINN PAPERS (2015).

are banally schematic categorizations which mirror the dichotomic thinking of ancient Western tradition, and arguably human beings' cognition processes more generally. Perhaps one might look at the holistic and oxymoronic pacification of opposites as traceable in Eastern philosophical praxis instead,[270] not to be kept hostage of empty, inconclusive, black-and-white linguistic bargaining which, in the cyber discourse, is leading us nowhere.

[270] NEUWIRTH, *supra* note 25, at 184–87.