TRILA in the Shadow of ‘National Security’: Towards Developing TWAIL Approaches to the International Law of Cyberspace

By:

Gunjan Chawla

October 1, 2020

In the 2020 Report of Teaching and Researching International Law (TRILA) Project by the Centre for International Law at the National University of Singapore, the international regulation of cyberspace has been counted among the least offered courses included in international law curricula—taught by only 8.7% of teachers attending. While cyberspace law remains a niche area in India generally, academic and civil society participation in the discourse around the social and political impact of digital technology is growing steadily.

At the Centre for Communication Governance at National Law University Delhi (CCG), we work on building capacity, and research, on issues relating to technology law and policy. An understanding of international law, and its

ongoing development to adapt to the cyberspace is crucial to our work. I lead the work of the Technology and National Security team at CCG, which is focused on the study of international law and cybersecurity, enabled by the generous support we receive from the William and Flora Hewlett Foundation. As a part of the Centre's capacity building and teaching mandate, we have developed a curriculum to teach 'Technology and National Security Law and Policy' to law students in India. I had the opportunity to re-design and teach this course at the National Law University Delhi, which happens to be my own *alma mater*.

This post is a dissection of the contents of and processes that culminated in my very first experience of teaching international law with a view to regulate cyberspace as a domain of conflict between States.

Approaches

Alongside teaching this course, my own research is aimed at developing Third World Approaches to International Law (TWAIL) approaches to cyberspace regulation. In this piece, and through this course, I have argued that if we can develop an appreciation for the potency of lawfare not only as a tool of coercion, but also as a tool of resistance to *status quo*, we will be able to wield it in a manner that enables us to create and perhaps even re-claim a certain operational and legal space for the goals and aspirations of the Third World in international legal institutions.

As a reflection of the dual purpose of my role at CCG, I write this piece with a dual intention. The first, as an academic in international law, is to open a conversation on 'lawfare' as a new area of inquiry in TWAIL theory. The second, as a practitioner in public policy, is to embark on an interdisciplinary exploration of how we can translate such TWAIL theories into practice through the Governments of developing nations, taking India as an example. However, given the socio-political milieu of India, headed by a strong nationalist Government that does not always wish to count itself among members of the 'Third World', it is an uphill task.

I believe that TWAIL approaches read with anthropologists Jean Comaroff and

John Comaroff's conception of lawfare and the work of Craig Jones on the juridification of war could help us better understand predominant definitions of lawfare. Comaroff and Comaroff define lawfare as "the resort to legal instruments, to the violence inherent in the law, to commit acts of political coercion, even erasure."

This stands in stark contrast to the more popular definition of lawfare put forth by Major General Charles Dunlap Jr, as "the strategy of using or misusing the law – as a substitute for traditional military means to achieve an operational objective". The latter definition, while taking a much narrower view of the various forms of coercion that States—especially Third World States—may be subjected to, choosing to focus solely on military action, functions on the assumption that 'lawfare is a weapon of the weak' and in doing so, conceals the historical, and contemporary experiences of the Third World with 'lawfare' waged by imperialist powers in the name of establishing the 'rule of law' in those jurisdictions. On the other hand, the Comaroffs' conceptualization of lawfare exposes this fatal flaw in Dunlap's definition by placing the smoking gun – law as weapon – in the hands of the colonial state (and not in the hands of colonial subjects) (Jones 2016).

And so, if we view the cyber norms processes through the lawfare lens, an exercise we undertook in Module V of our curriculum, it becomes apparent that adapting interpretations of international law in the cyber context in particular ways could severely intensify the coercive elements of internal and external sovereignty of Third World states, which often manifests as a disproportionate emphasis on 'national security and strategic interests' of the state. An exploration of the cyber norms processes through the lens of 'lawfare' should then, help us better appreciate the dynamic between older forms of (political) coercion through international law and legal institutions, and newer forms of (military) coercion made possible in and through cyberspace. Even though the term 'economic coercion' has yet to enter the parlance of cyber norms debate at the United Nations, the economic impacts of cybercrime on the balance of power and the historical amnesia of the West are also of great significance in this regard, as the United States' National Security Agency (NSA) termed cybercrime as the 'greatest transfer of wealth in human history'.

Background politics and research

In May 2019, India witnessed what has been dubbed as its first ‘national security’ elections. I wrote about how such an election agenda does not strengthen, but imperils national security institutions in a democracy.

By early 2020, India gained the unenviable distinction of becoming the most cyber-attacked nation in the world. Around the same time, the process to update India’s National Cybersecurity Policy first formulated in 2013 was initiated. CCG submitted a detailed dossier to the National Security Council Secretariat on the proposed National Cybersecurity Strategy for 2020-2025. It recommended, *inter alia*, the playing of a more proactive role in discussions at international fora involved in shaping rules, principles and norms for international law in cyberspace to protect its own strategic interests.

India has been a participant in the United Nations Group of Governmental Experts (GGE) as well as the Open-Ended working Group (OEWG), which are parallel processes to formulate international legal rules, norms and principles applicable in cyberspace that are ongoing within the United Nations framework. Opinions on the question of how international law applies in cyberspace begin to diverge, especially on the threshold for invocation of right to self-defence in cyberspace, as well as the application of international humanitarian law (IHL) in cyberspace. India has yet to take an explicit stance on the divide between the two camps, or articulate a middle ground.

The Indian Government’s assertions of sovereignty in cyberspace—faced with the onslaught of rhetoric surrounding ‘data colonialism’—continue to be projected inward onto its citizens, rather than towards the actual source of coercion and conflict in cyberspace. This is to say, that the coercive power of the state with reference to cyberspace in India is far more likely to manifest in expressions of *internal sovereignty* as opposed to *external sovereignty*. At a distance, this tendency appears to be shifting in recent times. Our curriculum design and content attempts to trace and critically analyze these apparent shifts.

Course design and structure

The curriculum for the Technology and National Security Law and Policy course is offered as an elective five-credit course to fourth and fifth year students of the integrated Bachelors of Arts and Law [B.A. LL.B. (Hons.)], a five-year program at NLU Delhi. It has been designed as an inter-disciplinary exploration of various themes in cybersecurity, with the formation and application of the international law of cyberspace at its core.

It is relevant to mention that students who joined this seminar course had already received instruction in a basic public international law as part of mandatory curriculum at the University. The course was conducted in 6 modules, and explored the role of technology in national security, as viewed from the standpoint of legal and international relations theory, strategy, international law and domestic law and policy. The design attempts to maintain a fairly similar, if not equal emphasis on divergent approaches to analyze (1) theory (2) strategy (3) regulation through Constitutional and domestic law and (4) regulation through international law.

A major challenge in compiling reading materials, specifically for Modules IV and V arose from my inability to access my office or library at the University campus and consequently, classical texts and other books in international law as well. This was of course, due to the country-wide lockdown in effect in the wake of the COVID-19 pandemic. Some of these readings will most likely be replaced in the next iteration of this course.

Nearly all assigned readings were either already available online, or were made available online to students. Classes for Modules II through VI were conducted entirely online. The full course outline and reading list can be downloaded here.

Course content and key learnings

Module I explored the concept of national security in a theoretical context and is intended as an introduction to basic concepts and ‘existential threats’ to define the limits and limitations of themes that fall within ‘national security’. It also highlighted the apparent tensions between national and international security and human rights law.

Module II was designed as an exploration of diverse theories in military strategy. The first part covered Western approaches, whereas in the second part we turned our gaze eastward to examine Chinese and Indian thinking, as well as Russian, to a limited extent. Works ranged from classical works of Sun Tzu and Clausewitz to more contemporary readings by strategists including Edward Luttwak and Richard Danzig. The most important contemporary reading from this module was from *Unrestricted Warfare*, a seminal text by two members of the People's Liberation Army (PLA) Col. Qiao Liang and Col. Wang Xiangsui.

An interesting outcome of this module was a re-calibration of students' perceptions of the work of Hugo Grotius who is widely considered to be the father of international law. Some of the papers submitted by students even argued that he would be better described as a strategist for the Dutch colonial expansion rather than an international lawyer.

Module III explored constitutional law and domestic legal provisions relevant for 'national security', an extra-constitutional term. This module started with the broad structure of national security institutions and constitutional provisions that can be invoked in times of emergencies before narrowing the focus to state surveillance and its tensions with the right to privacy.

Module IV added an extra-territorial dimension to the conversation on the State's power of surveillance to pivot the conversation to international law's apparent indifference the proliferation of foreign surveillance and cyber espionage activities among States in recent decades. Basics of *jus ad bellum* and *jus in bello* formed the other half of this module, wherein evolving interpretations of UN Charter provisions in the aftermath of the 9/11 attacks formed the centerpiece of this discussion, with an emphasis on the prohibition of the use of force and the inherent right of self-defence, which become extremely relevant in the cyber norms discussion.

Students also reported that the movie, *Eye in the Sky* (2015) recommended for viewing to students informally was a useful tool to illustrate a spectrum of coercive State behavior through espionage, sabotage, the use of military force and even targeted killings. It also supplied relatable context to understand the

practical complexities of a proportionality analysis under *jus in bello*.

Module V was focused exclusively on international law and cyberspace. The first part focused on the unique nature and attributes of cyberspace as a domain of State-to-State hostilities and the unique challenges it poses for IL regulation. The documentary *Zero Days* by Alex Gibney proved useful to explain the uniqueness of the cyber domain.

The second part of this module introduced the cyber norms processes currently underway at the United Nations, namely the Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) through the lens of lawfare. As disagreements to the manner in which international law applies to cyberspace persist among nations in practice, not only cyberspace, but also the framework of international legal regulation itself faces the risk of fragmentation into multiple factions that may not necessarily be compatible with each other.

In order to encourage critical thinking and problematize propositions often taken for granted, students were encouraged to reflect upon the sources of international law that apply in cyberspace and their legitimacy—including both editions of the Tallinn Manual—from the point of view of developing economies.

A pivotal component of this module was Professor B.S. Chimni's TWAIL critique of customary international law (CIL) that highlights CIL as a profoundly undemocratic source of international law. It also helped highlight the manner in which the re-interpretation of existing customary international law as applied in cyberspace would differentially impact developing economies. In this regard, the Tallin Manual's assertion that access to the internet is not a human right in itself emerged as a major point of the failure in Western treatments of the subject (Tallinn Manual, p. 195). We returned to examine this legal point in depth in the next module as well, while discussing the importance of access to the internet as internet shutdowns in India become more frequent.

Module VI returned the conversation back to domestic cyber law and policy to apply learnings from previous discussions to live issues such as debates on encryption, proliferation of spyware and associated risks for privacy and security and 'data sovereignty' as a concept distinct from but related to

‘sovereignty in cyberspace’.

In order to translate classroom discussions into good practices, the course culminated with a training session by a leading public interest technologist to familiarize students with tips, tricks and technological tools to ensure cyber security and practice cyber hygiene at the personal level. The abuse of governmental authority exercised in the name of national security, rather than in the interest of national security emerged as a key shared concern in these discussions.

The way forward

The design of this course is aimed at equipping young scholars from the Global South with the ability to appreciate the potent role of ‘lawfare’, potentially even as a tool of Third World resistance to the imperialism baked into international law and legal processes—at least in scholarship and theory, even if that is not their parent State’s actual practice.

If we can develop an appreciation of lawfare in practice as a tool at the disposal of states as well as non-state actors that has been instrumental in the construction of the contemporary international legal order generally, we will be able to better unpack the coercive elements of rules and help policymakers see merit in building agreement on specific questions with those who may be indifferent, or even averse to protecting our security interests. While agreeing with one’s adversary *in principle* may appear as a sign of weakness, agreeing *on a principle* already endorsed by the technologically superior adversary could enable the victim State to seek redress for violations of that agreed upon framework.

This course has been structured to be adaptable to the requirements that other academic institutions in India, or other jurisdictions may have. Primarily, course instructors from other legal systems and jurisdictions would need to replace the content of Modules III and VI, focused on domestic constitutional law and domestic cyber policy issues, respectively.

We at CCG welcome feedback and suggestions from the Afronomics/TRILA

community on the content, quality and clarity of the reading materials, as well their views on the suitability of the curriculum design to be adapted to the context-specific requirements in other institutions.

Gunjan Chawla is the Technology and National Security programme Manager at the Centre for Communication Governance at National Law University, Delhi. She was also a Judicial Fellow at the International Court of Justice in 2017-18.