International Review of the Red Cross (2022), **104** (920-921), 2077–2096.
How International Humanitarian Law Develops
doi:10.1017/S1816383122000285

IRRC

The crisis in international law and the path forward for international humanitarian law

Paul B. Stephan
Paul Stephan is the John C. Jeffries, Jr., Distinguished Professor of Law and the David H. Ibbeken '71 Research Professor of Law at the University of Virginia School of Law.
Email: pstephan@law.virginia.edu.

Abstract

This article offers a brief review of the forces that have contributed to the contemporary impasse in the formation of new international law and institutions. It identifies areas where development of the law of armed conflict would provide great benefits, yet where current international conditions render formal legal agreements highly unlikely. It then considers how to advance desirable projects nonetheless. In the absence of effective formal international law-making, jurists face a choice. One approach, which I call inspirational, is to propose idealized legal systems based on claims of justice and practicality. Much published work over the last decade seems to take this path. The hope is that the ideas will inspire and thus lead relevant actors to adopt the systems at a time when the obstacles to international agreements recede. The other approach, which I call entrepreneurial and describe here, involves leading States acting as "norm entrepreneurs". They can propound and in practice adhere to norms with the intention of inducing other States to follow. The entrepreneurial approach entails a State engaging in a practice that it hopes others will emulate, while the inspirational involves an appeal to the international community as a whole, including significant non-State actors.

Keywords: international humanitarian law, cyber-conflicts, non-international armed conflicts, norm entrepreneurs, international lawmaking.

Introduction

Across the board and around the world, projects to build international law and international institutions have become stuck. The liberal international consensus that seemed to emerge in the 1990s has unravelled.[1] The present moment of crisis has many causes – geopolitical, economic and cultural. What it means as a practical matter is that the formal adoption of new international rules through international agreements faces roadblocks that seem likely to persist for some time.

This article offers a brief review of the forces that have contributed to this impasse. It identifies areas where development of the law of armed conflict would provide great benefits, yet where current international conditions render formal legal agreements highly unlikely. It then considers how to advance desirable projects nonetheless. In the absence of effective formal international law-making, jurists face a choice. One approach, which I call inspirational, is to propose idealized legal systems based on claims of justice and practicality. Much published work over the last decade seems to take this path.[2] The hope is that the ideas will inspire and thus lead relevant actors to adopt the systems at a time when the obstacles to international agreements recede. The other approach, which I call entrepreneurial, and describe here, involves leading States acting as "norm entrepreneurs". They can propound and in practice adhere to norms with the intention of inducing other States to follow. The entrepreneurial approach entails a State engaging in a practice that it hopes others will emulate, while the inspirational involves an appeal to the international community as a whole, including significant non-State actors (the invisible college).[3]

Both approaches have advantages and shortcomings. The inspirational approach pushes toward idealized outcomes, but at the cost of indefinite delay and perhaps disenchantment. The entrepreneurial approach risks the emergence of divergent norms, perhaps dividing the world, as well as inaction. It also favours large States that find themselves facing certain legal issues more frequently than others. In the case of international humanitarian law, we are likely to see entrepreneurial rules favoured by States that project military force into conflicts, either international or non-international, rather than those

1 Paul B. Stephan, "Crises Come in Waves: National Populism, the Poisoning of Cyberspace, a New Cold War, and the Pandemic (2015-21)", in P. B. Stephan, *The World in Crisis and International Law – The Knowledge Economy, System Shocks, National Populism, and the Battle for the Future*, Cambridge University Press, Cambridge, 2022, forthcoming.

2 E.g. Ryan Goodman, "The Power to Kill or Capture Enemy Combatants", *European Journal of International Law*, Vol. 24, No. 3, 2013.

3 Martha Finnemore and Kathryn Sikkink, "International Norm Dynamics and Political Change", *International Organization*, Vol. 52, No. 4, 1998; Oscar Schachter, "The Invisible College of International Lawyers", *Northwestern University Law Review*, Vol. 72, No. 2, 1977.

preferred by States that find armed conflicts unfolding on their territory against their will. Until the consensus approach to international law-making becomes unblocked, however, this seems to be the best we can do.

This paper first describes present obstacles to the conventional international-law-making process by which States come together to make multilateral treaties regulating the conduct in question. It then identifies urgent issues in the law of armed conflict that cry out for regulation. These include rules governing non-traditional armed conflicts, understood as non-international armed conflicts (NIACs) involving armed force directed against a foreign State, and cyber-operations that threaten peace and security but fall short of the use of armed force. The paper describes what an inspiration approach to these issues might look like, and offers by way of contrast an entrepreneurial approach. It argues that not only does the latter approach offer greater promise over the short run, but it opens a path to greater international cooperation over the long run.

Why are we so divided?

The present moment finds the world as dangerously divided and on the edge of international violence as any in the last thirty years. One set of threats involves geopolitical issues, largely those that the end of the Cold War buried but did not settle. Russia's role in the post-Soviet space and the reunification of the two Chinas highlight the list. These threats in turn reflect economic conflicts arising from the breakdown of the liberal internationalist regime put in place in the 1990s. These political and economic challenges have led important States to reject the current international order and called for significant revision of international relations and law. The other set of threats involves the emergence of cyberspace as a place of danger and a platform for harmful acts. These developments have polarized the world, with one camp seeking to defend what they believed was the post-Cold War settlement and the other challenging the contemporary international order.[4]

There are as many explanations for the troubles of the present as there are observers. I offer here a stylized and truncated narrative that focuses on two factors: (1) geopolitical changes related to the use of force in international and non-international disputes, and (2) the achievements of information technology. This is not the entire story, but my account provides a basis for thinking about the future of international humanitarian law.[5]

Geopolitical issues and non-traditional armed conflicts

The end of the Cold War, a moment that began with the June 1989 Polish election that brought the opposition to power and ended with the dissolution of the Soviet

4 President of Russia, "Joint Statement of the Russian Federation and the People's Republic of China on the International Relations Entering a New Era and the Global Sustainable Development", 4 February 2022, available at: http://en.kremlin.ru/supplement/5770 (all internet references were accessed in April 2022).

5 In this section I draw substantially on my forthcoming book. P. B. Stephan, above note 1.

Union in December 1991, seemed to put an end to the bipolar regime that had governed international security issues since the Second World War. This opened the door to the possibility of a new world order based on the international rule of law. It became possible to imagine a world where international uses of armed force would rest on international consensus, reflected in the actions of the United Nations Security Council, and thus increasingly rare.

An episode occurring right at the end of the Cold War gave people hope about the use of international law as a constraint on the international use of force. Following Iraq's conquest and purported annexation of Kuwait in 1990, the Security Council assumed jurisdiction over the dispute and authorized the international community to use "all necessary means" to resolve it. The subsequent liberation of Kuwait and the imposition of reparations and international supervision on Iraq received the support of the Soviet Union and China, through assent in the case of the former and abstention on the part of the latter.[6] Worldwide, States walked away from the bipolar structure that had dominated international relations for the previous forty years. Many thoughtful people believed that we found ourselves in a new age of collective security and democratic peace with the international rule of law and peaceful resolution of international disputes replacing the threat of armed conflict and the risk of Armageddon.[7]

Over time, however, the hopes these events raised seemed increasingly hollow. After 1991, armed conflict did not disappear, but shifted. Some wars of national liberation ended with real political change and an end to organized violence, as in South Africa. However, new conflicts, increasingly of a non-international nature, proliferated. The breakup of Yugoslavia was an early illustration: disintegration of the big State led to conflict among the component States that popped up in its place, but the worst of the fighting took place within Bosnia-Herzegovina and Serbia (with respect to Kosovo). Russia's terrible civil war in Chechnya provides another example of a consequential NIAC during this time. The festering wound that is the Palestinian–Israeli conflict got worse during the 1990s, and the breakup of Ethiopia produced atrocities. Overall, we saw very few incidents of war only between States, but a growing number of entrenched and dangerous armed conflicts within States.

Then came the events of 11 September 2001 (9/11) and the forever wars that they spawned. Mass terror attacks in the rich world, Madrid, London and Paris as much as New York, changed the mentality of many people and provoked responses that looked more like traditional international conflict. Coalitions invaded and conquered Afghanistan and Iraq, the former with the Security Council's approval and the latter without. The invaders discovered that conquest did not result in triumph, but instead in prolonged insurgencies that in many

6 United Nations Security Council, Security Council Resolution No. 678, 29 November 1990.

7 E.g. *Francis Fukuyama, The End of History and The Last Man*, Hamish Hamilton, London, 1992; Bruce Russett, *Grasping the Democratic Peace: Principles for a Post-Cold War World*, Princeton University Press, Princeton, NJ, 1993.

ways resembled the old wars of national liberation. In 2011 States reprised this behaviour by choosing sides in Syria's civil war, a US-led coalition invoking a right to collective self-defence against non-State organizations operating on the territory of Syria and Russia and Iran introducing forces at the invitation of Syria's government.

These events illustrate what I call non-traditional armed conflicts. These are NIACs that are neither anti-colonial struggles of national liberation nor civil wars confined to the territory of a State. Rather, they involve armed struggle by non-State actors to bring about a regime change in a particular State or region that extends outside the borders of the contested territory. Organizations such as Al-Qaeda and Da'esh embody non-State parties to such conflicts, as did the Liberation Tigers of Tamil Eelam in an earlier day.

The cyber-revolution and international conflict

Around the same time as the end of the Cold War, information technology underwent a revolution. People already had e-mail, list-servs and online databases, but these tools were somewhat clunky and mostly for "wonks". Then in 1994 we got Netscape Navigator, the first general-use web navigator, and the internet became a thing. Suddenly just about everyone had a portal to cyberspace, a wonderful world with an amazing range of images, sounds and writing. Not much more than a decade later we had smart phones and social media that further democratized connections and influence around the world through cyber-activity. These developments transformed our world.

The cyber-revolution, an explosion in connectivity that increasingly allowed people to bypass central authorities to communicate, agitate and organize, unfolded during the first decade of the present century. Visionaries imagined a new world of bottom-up democracy that would bring to account corrupt authoritarian regimes as freedom spread from the virtual space to the physical space. Grass-roots protest campaigns aided by the new technologies ousted leaders in Georgia, Ukraine, Kyrgyzstan, Tunisia, Libya and Egypt. A new world of people power seemed to be being born. Cyber-tactics could defang authoritarian uses of targeted force by enabling elements of surprise and swarming for popular uprisings that resist State-sponsored suppression of protests. The cyber-revolution, in the eyes of some, represented the death knell of violent authoritarian regimes and thus provided yet another path to a democratic peace.[8]

The 2011 Arab Spring, while embodying the potential of the internet revolution, also came to show how these hopes could come to nothing.[9] In some instances, incumbents were overthrown, but in the majority of places, ruling

8 E.g. Malcolm Gladwell and Clay Shirky, "From Innovation to Revolution: Do Social Media Make Protests Possible?", *Foreign Affairs*, Vol. 90, No. 2, 2011.

9 Zeynep Tufekci, *Twitter and Tear Gas: The Power and Fragility of Networked Protest*, Yale University Press, New Haven, CT, 2017.

regimes held off insurgents. All told, the outcome was mostly a mixture of failed States and humanitarian disasters, rather than reformed societies run by free peoples. Schooled by the fate of their unfortunate peers, authoritarians increasingly exploited the new technologies to surveil and remove their adversaries. Once an instrument of liberation, cyberspace increasingly became the place where States bolstered their defences against dissidents.

The same technologies that gave States greater resources to leverage domestic social control also provided new instruments for prosecuting international conflicts. The tools used to surveil domestic opponents also unlocked foreign databases. Cyber-actors (whether acting on behalf of a State or as independent predators) can disable online systems so as to degrade or destroy their functionality or hold them hostage against ransom. These actors also can infiltrate online media so as to engage in disinformation and psychological warfare. The cyber-tools not only greatly multiply the efficacy of these interventions, but complicate attribution of responsibility. These malign capacities exacerbate both traditional international disputes and the prosecution of non-traditional armed conflicts.

Challenges for international humanitarian law

As the 2020s unfold, it becomes increasingly clear that the liquidation of a bipolar international order did not mean the end of devasting armed conflict, and that the information revolution benefitted incumbents wielding State power at least as much as reformers pushing for freer and less corrupt societies. Both developments breed instability and leverage threats to peace and prosperity. They also raise issues related to international humanitarian law.

With respect to non-traditional armed conflicts, the legal issues include the legal status of people taking part on behalf of non-State actors through extraterritorial attacks. Neither the international humanitarian law applicable to NIACs nor that applicable to international armed conflicts offers a clean fit. Issues arise, such as the status of combatant privilege, culpability for the provision of material assistance, and the existence of a power to detain during hostilities, but satisfactory responses under existing law do not.

A concrete example may serve as an illustration of a general class of problems. Under Article 110 of the Third Geneva Convention, incurably wounded or sick detainees enjoy a right of repatriation. In the case of NIACs, neither the Convention nor the two Additional Protocols address repatriation. In many instances, a person detained in a NIAC is likely to be a national of the detaining power. But in non-traditional conflicts where armed conflict extends to States of which the non-State actors are not nationals, detention may occur somewhere other than the participants' homeland. Yet those detained persons do not serve on behalf of their State of nationality, as participants in an international armed conflict do, and may face severe repercussions were they returned home. How does the principle underlying Article 110, regarding the release from

confinement of persons who, based on medical considerations, no longer present a realistic possibility of a return to combat, apply in such cases?[10]

As to cyber-operations, very little international law exists except by way of analogy. Many experts believe that cyber-activity that produces significant material harm to persons and physical things remains subject to international humanitarian law. Thus, crashing an aircraft through means of cyber-intervention would come under this regime. Other general principles of international law such as non-interference presumably apply, although how and to what exactly remain open questions. The law applicable to operations that cause economic but not physical harm, including the destruction of online stored data, is disputed.

To take a salient example, in recent years, increasingly malicious cyber-activity has popped up around the world. Predators either seize control over stored data to shut down normal operations or threaten to make that data public. Attribution of these attacks is unclear, but States subject to them sometimes claim that they emanate from States with which they have geopolitical or even armed conflicts. The disabling of Ukrainian official websites during January–February 2022, a prelude to the later armed invasion and occurring during an ongoing armed conflict between Russia and Ukraine in Ukraine's Donbas Region, is a recent instance.[11]

The problems that we face

The world faces many threats that require collective action for an effective response. Climate change, proliferation of weapons of mass destruction, and future pandemics, including those deliberately engineered using cutting-edge technology, may lead the list. We have not seen, but surely can anticipate, the falling of terrible weapons into the hands of non-State actors. Pressing problems in the law of armed conflict also demand our attention and cry out for responses.

This background of growing international tensions and anxieties gives salience to particular issues of international humanitarian law. I focus here on two sets of issues that reflect the transformations in international conflicts and technology that the previous section describes. First, over the last two decades, we have seen an increase in the gravity and prevalence of non-traditional armed conflicts that challenge established concepts such as State involvement and military formations. We need clarity on the rules that bind States as they engage in such conflicts, whether through direct military operations or through

10 See *Al-Qahtani v. Trump*, 443 F. Supp. 3d 116 (D.D.C. 2020) (interpreting Army regulation as implementing Article 110 with respect to Guantanamo detainee).

11 I recognize that some eminent jurists question whether Russia and Ukraine were engaged in an international armed conflict before 24 February 2022. E.g. Bakhtiyar Tuzmukhamedov, "Law is Not Silent, Even When the Guns Speak", *Nezavisimaya gazeta*, 9 March 2022, available at: https://www.ng.ru/kartblansh/2022-03-09/3_8386_kb.html. The Russian Federation also rejects the characterization of the post-24 February operations in Ukraine as an invasion. I reach the characterizations in text based on my own assessment, appreciating that my conclusions may be controversial in some quarters.

supporting non-State actors, as well as those constraining non-State actors directly. Second, we also need rules governing international cyber-operations, not just those that bring about physical violence but those that cause serious economic or personal harm.

Non-traditional armed conflicts

Recent decades have taught us that both States and organized groups can employ force at a large scale, but not in forms that the traditional law of armed conflict addresses. Non-State actors seeking to bring about regime change can use force to attack States that they perceive as supporting their adversary. The 9/11 (New York), 11 March 2004 (Madrid), 7 July 2005 (London) and 13 November 2015 (Paris) attacks are exemplary. In response, States increasingly use military resources to identify and attack adversaries while relying on analogies rather than rules to determine who may qualify as a lawful target. Increasingly they use remote weapons such as drones, which by limiting the range of violence may be more precise than traditional weapons but not necessarily more accurate, in the sense of finding the intended target. The fiasco during the US evacuation from Hamid Karzai International Airport in August 2021, when a US drone slaughtered a family mistakenly targeted as insurgents deploying an armed attack, illustrates the humanitarian risks of such operations. The attack did not go off course, but the means of determining who was to be killed were flawed.[12] Other issues, among many, include the power to detain participants in these conflicts who are not part of formal military structures and the duties owed to detainees. The host of questions surrounding the Guantanamo detention issue, including the Article 110 question discussed above, illustrate the incompleteness of current international humanitarian law in the face of pressing problems.

At the moment, treaties addressing the law governing NIACs include Article 3 common to the four Geneva Conventions and the 1977 Additional Protocol II.[13] Even many strong proponents of these instruments would admit that they contain large gaps as well as significant interpretive problems, including fundamental questions of jurisdiction. Moreover, important States have not joined the Additional Protocols. People looking for more law can invoke

12 An initial review of the incident carried out by the US Air Force inspector general concluded that the threat entailed no violation of law, including the law of war, but that "[e]xecution errors combined with confirmation bias and communication breakdowns led to regrettable civilian casualties." See "Investigation into 29 Aug CIVCAS in Afghanistan", *Washington Post*, 3 November 2021, available at: https://context-cdn.washingtonpost.com/notes/prod/default/documents/b72be59f-f01e-4e3a-bdba-8582472b9c83/note/25812926-b3ca-4280-9e69-2e337a8d6a23.#page=1. For more on the incident and the investigation, see Alex Horton, Dan Lamothe and Karoun Demirjian, "Botched Drone Strike That Killed 10 Civilians in Kabul Was Not a Result of Criminal Negligence, Pentagon Says", *Washington Post*, 3 November 2021, available at: https://www.washingtonpost.com/national-security/2021/11/03/kabul-drone-strike-inspector-general-report/.

13 Other treaty regimes, such as the Rome Statute, also may apply, although jurisdiction over non-parties might require a decision of the Security Council. In the case of the Rome Statute, very few States that regularly engage in armed conflict outside their own territories are State parties.

customary rules.[14] Yet fierce debates persist over the standards for finding and enforcing customary international law in the realm of armed conflict.[15]

I have no desire to adjudicate those disputes here. Rather, my point is that, even when the dust settles in the fight over the scope and meaning of treaty and customary law, few believe that we have as fully developed and clearly formulated international law governing the ramifications of non-traditional armed conflicts as we would wish. If one thinks, as I do, that we can expect more and greater conflicts of this sort in the near future, then one should wish for a law-making project to plug the gaps in the *lex lata*, whatever one believes the *lex lata* to be.[16]

However, the growing mistrust and adversarial nature of international relations, especially among States most likely to find themselves taking part in a non-traditional international armed conflict, make prospects for treaty formation decidedly bleak. States may reject an otherwise useful formulation of international law if they conclude that such a rule might benefit their adversaries more. They will invest more in maintaining their adversary status than in finding common ground.

A complicating factor is the lack of reciprocity that might otherwise drive States toward cooperation. Conventional NIAC by definition excludes a situation where States find their military organizations directly opposed in a conflict. In a non-traditional NIAC, the non-State adversary, which may or may not receive aid and comfort from other States, typically seeks to challenge more than one particular State regime. The conflict necessarily occurs on the territory of one or more sovereign States, but the State where much of the armed force originates may have little or no capacity to affect events.[17] These non-State actors lack a place at the bargaining table and indeed mostly lack a structure that enables them to make credible commitments through international agreements. Lack of coordination among non-State actors, as illustrated by the present conflict in

14 Jean-Marie Henckaerts and Louise Doswald-Beck (eds), *Customary International Humanitarian Law*, Vol. 1: *Rules*, Cambridge University Press, Cambridge, 2005 (ICRC Customary Law Study), available at: https://ihl-databases.icrc.org/customary-ihl/eng/docs/v1.

15 Dennis Mandsager, "U.S. Joint Letter From John Bellinger III, Legal Adviser, U.S. Department of State, and William J. Haynes, General Counsel, U.S. Department of Defense to Dr. Jakob Kellenberger, President, International Committee of the Red Cross, Regarding Customary International Law Study", *International Legal Materials*, Vol. 46, No. 3, 2007, p. 514; republished as John B. Bellinger, III and William J. Haynes II, "A US Government Response to the International Committee of the Red Cross Study *Customary International Humanitarian Law"*, *International Review of the Red Cross*, Vol. 89, No. 866, 2007, pp. 444–5; W. Hays Parks, "The ICRC Customary Law Study: A Preliminary Assessment", *American Society of International Law Proceedings*, Vol. 99, 2005, p. 212; see W. Hays Parks, "Part IX of the ICRC 'Direct Participation in Hostilities' Study: No Mandate, No Expertise, and Legally Incorrect", *New York University Journal of International Law and Politics*, Vol. 42, 2010, p. 784 (criticizing Part IX of Nils Melzer, *Interpretive Guidance on the Notion of Direct Participation in Hostilities Under International Humanitarian Law*, ICRC, Geneva, 2009, available at: https://www.icrc.org/en/doc/assets/files/other/icrc-002-0990.pdf).

16 I note here the argument of Samuel Moyn that we should spend less time worrying about the *jus in bello* and look instead to ways to bar use of force in international relations altogether, whether more humane or not. Samuel Moyn, *Humane: How the United States Abandoned Peace and Reinvented War*, Farrar, Straus and Giroux, New York, 2021, pp. 267–311.

17 Ashley S. Deeks, "'Unwilling or Unable': Toward a Normative Framework for Extraterritorial Self-Defense", *Virginia Journal of International Law*, Vol. 52, 2012.

Syria and the forces that expelled the United States-led coalition from Afghanistan, illustrate this. Where bargaining with non-State actors is impossible or extremely difficult, States are not inclined to make concessions to restrict their actions. Under these conditions, we cannot expect new international agreements on the rules governing armed conflict to emerge.

I do not mean to suggest that compliance with international law necessarily requires a prospect for reciprocity. International humanitarian law, for example, rejects reciprocity as a general matter, including a suspension of obligations as a countermeasure.[18] Other factors can explain rule adherence in international relations.[19] States make human rights commitments, for example, without any expectation of reciprocity.[20] My point is that, if compliance is costly because it requires a State to give up something that it wants to do, States in general would be less likely to assume and honour international obligations when they expect general non-compliance, and that the lack of possibilities for reciprocity removes a factor that would support an expectation of compliance.

Cyber-operations

When we turn from non-traditional armed conflicts to cyber-operations, we find even fewer legal instruments that might constrain State behaviour.[21] No multilateral treaties address the issue. Some debate whether general instruments, such as the United Nations Charter, the Geneva Conventions, or the International Covenant on Civil and Political Rights, might provide a few rules of the road, but nothing like a consensus exists around this proposition.[22] Instead,

18 Vienna Convention on the Law of Treaties, 23 May 1969, 1155 UNTS 331, Art. 60(5).

19 Paul B. Stephan, "Enforcement of International Law", in Francesco Parisi (ed.), *Oxford Handbook of Law and Economics*, Vol. 3: *Public Law and Legal Institutions*, 2017.

20 Whether States comply with these commitments is another matter. Oona A. Hathaway, "Do Human Rights Treaties Make a Difference?", *Yale Law Journal*, Vol. 111, 2002.

21 I do not address here another lurking problem with cyber-operations, namely the applicability of the *jus ad bellum*. As I have written elsewhere, one might worry that the understandable desire of international lawyers to use the *jus in bello* to limit the harms of these operations might evolve into an argument that these operations qualify as acts of armed force that justify armed non-cyber-responses. The evolution is not inevitable, but neither is it implausible. Paul B. Stephan, "Big Data and the Future Law of Armed Conflict in Cyberspace", in Matthew C. Waxman and Thomas W. Oakley (eds), *The Future Law of Armed Conflict*, Oxford University Press, New York, 2022. See S. Moyn, above note 16.

22 E.g. Australian Ministry of Foreign Affairs, *2019 – Supplement to Australia's Position on the Application of International Law to State Conduct in Cyberspace*, available at: https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/LawStatements/2019+Supplement+to+Australia_s+Position+on+the+Application+of+International+Law+to+State+Conduct+in+Cyberspace.pdf; French Ministry of the Armies, *International Law Applicable to Operations in Cyberspace*, available at: https://www.dropbox.com/s/rco3345z42b1em3/Application%20of%20International%20Law%20to%20Cyber%20Operations%20_%20The%20Hague%20Program%20for%20Cyber%20Norms%20_%20March%202020%20incl%20ANNEX.pdf?dl=0; Government of the Kingdom of the Netherlands, *Report to Parliament, Appendix: International Law in Cyberspace*, available at: https://www.dropbox.com/s/rco3345z42b1em3/Application%20of%20International%20Law%20to%20Cyber%20Operations%20_%20The%20Hague%20Program%20for%20Cyber%20Norms%20_%20March%202020%20incl%20ANNEX.pdf?dl=0; New Zealand Office of the Prime Minister and Cabinet, *The Application of International Law to State Activity in Cyberspace*, available at: https://dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20 State%20Activity%20in%20Cyberspace.pdf; for Germany, The Federal Government, *On the Application of*

what we find are aspirational, and fairly amorphous, statements by expert committees commissioned by the United Nations, alongside State-initiated but independent expert studies, of which the *Tallin Manuals*, organized but not endorsed by the North Atlantic Treaty Organization (NATO), are the most prominent.[23]

A number of States, including Australia, France, Germany, Israel, the Netherlands, New Zealand, the United Kingdom and the United States, have produced statements from leading government lawyers expressing views on the application of international law to cyber-operations.[24] A careful analysis of the statements, however, reveals cautious wording designed to avoid specific commitments as to international law alongside general claims about the existence of customary international law. Illustrative is the French statement, which discusses the principle of sovereignty as a limitation on foreign State operations against another State. Although ambiguous, it seems to conclude that "the decision whether or not to respond to such operations is a political one, taken in light of the nature and characteristics of the intrusion".[25] The point, suggested rather than stated, is that the principle of State sovereignty enshrined in the United Nations Charter does not on its own produce any legally enforceable rules governing cyber-operations.

Again, my goal is not to pick and choose among the projects and pronounce on where a sufficient consensus exists to justify a conclusion about particular rules of customary international law. My observation, rather, is that many of the States in the so-called "West" have made statements that might indicate that a body of customary international law governing State actions in cyberspace exists, but that the views of other States are less clear and that even the States that have made declarations agree on few if any specific rules.

This sparsity of law persists in the face of an apparent uptick in offensive cyber-operations during the COVID pandemic.[26] I must say "apparent" because

International Law in Cyberspace, available at: https://www.auswaertiges-amt.de/blob/2446304/2ae17233b62966a4b7f16d50ca3c6802/on-the-application-of-international-law-in-cyber-space-data.pdf; Roy Schorndorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, available at: https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; for the United Kingdom, Jeremy Wright, *Cyber and International Law in the 21st Century*, available at: https://www.gov.uk/government/speeches/cyber-and-international-law-in-the-21st-century; for the United States, Brian J. Egan, "International Law and Stability in Cyberspace", *Berkeley Journal of International Law*, Vol. 35, No. 1, 2017; for the United States, Paul C. Ney, Jr., "Some Considerations for Conducting Legal Reviews of U.S. Military Cyber Operations", *Harvard International Law Journal*, Vol. 62, 2020.

23 United Nations General Assembly, Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, UN Doc. A/76/135, 14 July 2021; Michael N. Schmitt (ed.), *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, Cambridge, 2013; Michael N. Schmitt (ed.), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2017.

24 See sources, above note 22.

25 French Ministry of the Armies, above note 22, p. 7.

26 E.g. Jenny Jun and Nadiya Kostyuk, "The Pros and Cons of Mandating Reporting From Ransomware Victims", *Lawfare*, 1 November 2021, available at: https://www.lawfareblog.com/pros-and-cons-mandating-reporting-ransomware-victims.

we know only about attacks that governments have acknowledged, attribution of particular attacks to State actors remains contested, and we have every reason to believe that many State-sponsored operations, especially those dedicated to espionage rather than to inflicting economic or social costs, go undisclosed. Moreover, many of these attacks seem the product of geopolitical tensions but not necessarily within armed conflicts. The concern is that, were we to see more armed conflicts, such as the conflict between Russia and Ukraine currently under way, we also would see more of these operations.

Still, we have seen a growing number of civilian activities compromised by suspicious operations in a context where adversary State involvement is suspected, if not proved. An illuminating example is a tit-for-tat exchange between Israel and Iran in the autumn of 2021 in the context of an ongoing, if undeclared, armed conflict between Israel, Hezbollah and Iran. According to the New York Times, Israel undertook an operation that shut down the retail automobile petrol distribution system in Iran for the better part of the week, leaving drivers in the lurch. Iran retaliated by hacking Israel websites catering to unconventional sexual practices and then released private and embarrassing information regarding a number of persons, some prominent but unconnected to the government.[27] If one may believe the reporters, both States used civilian targets as a means of prosecuting a State-to-State dispute, in each case employing measures that cannot easily be analogized to acts of force but that do entail considerable economic or moral cost.

As the offensive capacities of cyber-operations grow, the need for constraints seems evident. The more economic and social life moves online, the greater the need for security. We already have seen instances of essential medical services shutting down due to ransomware attacks.[28] The prospect of crashing financial markets and services, perhaps alongside erasure of financial records, seems to pose a real and substantial threat. Surely, we can find rules that discourage States from launching cycles of action and reaction that generate increasingly burdensome costs on civilian populations, even if the effects are rarely lethal or even physically damaging.

At first sight, reciprocity would seem a good foundation for such agreements. States function as both perpetrators and victims of cyber-operations, and not all operations are carried out by States. Obligations on States to reduce harmful consequences would lower the risk of symmetrical attacks by States that bear the obligation. Win-win deals await.

However, roadblocks to formal agreement remain. First, the blurred lines between public and private in advanced cyber-technology make it extremely difficult to tell when a State should bear responsibility for an operation, just as secrecy and immateriality in cyber-operations complicate attempts to determine

27 Farnaz Fassihi and Ronen Bergman, "Israel and Iran Broaden Cyberwar to Attack Civilian Targets", *New York Times*, 27 November 2021, available at: https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html.

28 Danielle Gilbert, "Ransomware Lessons for a Nation Held Hostage", *Lawfare*, 12 September 2021, available at: https://www.lawfareblog.com/ransomware-lessons-nation-held-hostage.

which State took part in an attack.[29] Without some effective mechanism of holding States to account for cyber-operations, rules are meaningless. But not all bad things that happen in cyberspace rest on acts of State. In some cases, criminal gangs carry out costly actions – ransomware comes to mind – without any State involvement, or at most State indifference. In others, people take the tools developed while working for the State and deploy them for their own purposes. In yet others, people working in State cyber-organs end their official workday and then switch into private mode, using skills and tools attributable to the State to carry out their own projects. An analogy to the old letters of marque and reprisal comes to mind.

Second, States have fundamentally perverse incentives in the carrying out of cyber-operations. As technology has transformed the world, the capacity to undertake offensive activity in cyberspace has become as important as old-fashioned kinetic capability. The fast-changing technology requires practitioners to constantly update their skills, which requires practical experience and experimentation. Restraints cut back on the ability to innovate. This applies as much to defence as offence: a reduction in threats due to State compliance with agreed standards puts persons charged with cybersecurity to fewer tests. As technologists, people who work in cyberspace find formal limits at odds with the fundamental dynamic of their work.

Third, restraint favours defence, yet the fundamental dynamic in the evolution of cyber-capabilities favours offence. If we imagine cyber-operations as a game pitting offence – the authors of the operation – against defence – those seeking to protect information security and frustrate intrusions, the rewards skew heavily in the direction of offence. The authors of an operation know their target and appropriate all the benefits of their success, whether monetary, prestige or power. Defenders must anticipate and take costly measures to lower risks that may never materialize. They seldom get direct benefits from their success in thwarting attacks, even though society as a whole benefits. Rather, they only get to live to fight another day. In theory, States should not care about such incentives, as they are set up to attend to the general welfare – what economists call public goods. Yet States are made up of human beings to whom incentives are meaningful. Accordingly, any international agreements that restrict cyber-operations cut against the grain of the workers who populate these fields.

None of these is an insoluble problem. Indeed, much of the law of armed conflict faces similar dynamics and yet does its job well enough. The first obstacle, however, is specific to cyber-operations – attribution and rules of State responsibility. Cyber-technology over the last fifty years, if not longer, evolved as private activity comprising both profit and non-profit sectors unfolding alongside government-directed research and development. The mix varies over time and in different countries, but almost nowhere does world-class cyber-capability, either offensive or defensive, reside exclusively in State organs.

My general point is that State attribution of cyber-operations arises across a spectrum of activities, from those carried out directly by State organs to those

29 Kristen E. Eichensehr, "The Law and Politics of Cyberattack Attribution", *UCLA Law Review*, Vol. 67, 2020.

employing resources procured from the State to those where a State simply does not do enough to stop private activity. We cannot have rules regulating cyber-operations without deciding on what point along the spectrum does a State become answerable for what happens. Moreover, we would need to agree on rules of evidence, including presumptions and permissible inferences, to close the gap between observed behaviour and legal assessment.

Building international consensus around such rules seems unrealistic in the absence of high levels of trust and a great sense of urgency. Once one rejects the two poles of the spectrum – State immunity and strict liability – convergence on any particular mix of attribution and evidentiary rules would require a flexibility and a willingness to assume risks of unwanted outcomes that we simply do not see in today's world. Each of the relevant States in the world of cyber-operations would look at proposals not in terms of overall global benefits, but rather in terms of relative advantage for itself compared to its adversaries. As long as this perspective dominates, agreement seems impossible without a revolutionary change in circumstances or the lapse of a long time.

In sum, the road to formal agreement on rules for non-traditional armed conflicts and international cyber-operations for the present time seems blocked. The remainder of this paper considers what alternatives we might have to bypass the obstacles. These alternatives are, I argue, on the one hand good accounts of where we want to end up and, on the other hand, unilateral State practice that might lead others to follow. The next part describes how the inspirational approach might take on the problems of non-traditional armed conflicts and harmful cyber-operations in the context of armed conflicts. It then compares how an entrepreneurial approach to these issues might play out.

Pathways to new international humanitarian law

Thus far I have identified two areas where more international humanitarian law would be desirable – regulation of non-traditional armed conflicts and the use of cyber-operations in all kinds of armed conflicts – and explained why we should not expect conventional international law-making in these areas any time soon. In this section I compare and contrast the inspirational and entrepreneurial approach to these problems and suggest particular outcomes that might be obtainable.

The inspirational approach

In the United States, we have this phrase, borrowed from a W. P. Kinsella novel: "If you build it, they will come."[30] It is a vivid expression of the concept of socialization:

30 W. P. Kinsella, *Shoeless Joe*, Houghton Mifflin, Boston, MA, 1982. Not only the United States: Kinsella was Canadian. I appreciate that many readers may know this phrase from the movie *Field of Dreams*, rather than from the book on which the film was based.

articulation of a social norm can bring about emulation, independent of any direct rewards and punishments to induce conformity. People need to know that the norm seems desirable and that others will regard it as such. If they believe the second thing, they will comply so as to avoid others perceiving them as anti-social. People value acceptance, so a norm can achieve compliance simply by convincing people that others will esteem them more if they conform.[31]

From this perspective, the best way to bring the world more and better law, including that governing armed conflicts, is to make good proposals. An intelligent, reasoned and persuasive account of why a set of rules will make the world a better place will lead relevant actors to adopt it. It will not matter if the particular actor is unconvinced by the case for the rules as long as it concludes that other relevant actors will be. Desiring inclusion and abhorring others regarding it as a bad actor, the State will embrace the proposal. Naturally, some States will embrace the role of norm-breaker. But as long as most States adhere, the acts of deviance will reinforce and clarify the norm.[32]

The principal tools of the inspirational approach to international law-making are words, typically written. To inspire, a proponent of a norm needs an account as to why certain practices or values will make the world better. These accounts can come not only from States, but perhaps even more from non-State actors, including organizations such as the International Committee of the Red Cross (ICRC). Non-State actors can argue that their narrative reflects the general interests of the international community, and not the narrow interests of a particular State. They can make clear what might be latent and subject to doubt, that a particular rule will benefit all and that the State that embraces it will show to the world that it is estimable and benign.

My casual impression is that a large portion of the *jus in bello* scholarship published in English conforms to this model.[33] The effect of socialization is more assumed than stated. Scholars believe that intelligent, reasoned and persuasive proposals are good, without necessarily asking how they will influence State behaviour. Projects like the *Tallin Manuals* exemplify the approach. They rest on a belief that independent experts enjoy a degree of respect and deference that leads official actors to give them a fair hearing. If the hearing goes well, they can expect the official actors to conclude that States generally will buy into the proposal and that they must go along to avoid an unwanted outsider status.

31 Ryan Goodman and Derek Jinks, *Socializing States: Promoting Human Rights Through International Law*, Oxford University Press, New York, 2013.

32 See, generally, on the social function of deviance, Kai Erikson, *The Sociologist's Eye: Reflections on Social Life*, Yale University Press, New Haven, CT, 2017, pp. 28–9.

33 And not only *jus in bello* scholarship. For a paradigmatic example of the inspirational approach at work in the realm of human rights law, see *Jurisdictional Immunities of the State (Germany v. Italy, Greece Intervening)*, International Court of Justice Reports, 3 February 2012, Dissenting Opinion of Judge Cançado Trindade (focusing on publications and conference declarations rather than State acts and explanations), available at: https://www.icj-cij.org/public/files/case-related/143/143-20120203-JUD-01-04-EN.pdf.

It is easy to understand why non-governmental organizations of experts would find this perspective attractive. The ICRC, as the foremost such group in the field of international humanitarian law, in particular should embrace it. And, all in all, what is wrong with intelligent, reasonable and persuasive arguments?

The short answer, I think, is that there is nothing wrong with good proposals as long as one appreciates their limits. The premise of the socialization argument, drawn from sociology, is that the international community is every bit as much a society as are other social structures and that nations are as averse to being perceived as anti-social as are people. In times of peace and prosperity, this may make sense. But during periods of political and technological upheaval and growing uncertainty about and alienation from group norms, socialization may do less work than is supposed. More States may define themselves as revisionist in the face of perceived injustices and dysfunction in the international order. These States may seek not simply to deviate from widely accepted norms but to pursue systemic disruption so as to implement a new and different order.

If one believes that the state of the world today is more divided than connected, then marking out one's place along the fault lines may matter more than gaining acceptance. Revisionist regimes may regard their grievances as more significant than their common interests. These actors will resist even reasonable proposals if they regard embracing them as a sign of weakness and a distraction from their overall project of restructuring international relations, not by reason but through power and persistence.

I think we live in such a world today. If I am right, then whatever we build, they will not come for a long time. At a minimum, the proposals would be historically premature.

The problem is not just delay, however. The longer a proposal goes unadopted, the easier it is for people to conclude that the community regards it as lacking social value. This is socialization's symmetrical downside: when enough time lapses, a proposal that does not get taken up becomes an indicator not of other-regardingness, but of the opposite. A State would not join even if it liked the proposal, if it believed that other actors would regard the embrace as anti-social.

Under these conditions, inspiration would be counterproductive and new rules would not emerge. Even international norms that might provide general benefits across conflicting blocs would not gain traction. One side's embrace of a rule as a sensible solution to a general problem would be seen by the other side as a projection of its values and narrative and therefore as unacceptable, however sensible it otherwise might be.

The entrepreneurial approach

The alternative path to the development of an international legal order is to lead by example. A State may insist on a norm that it knows that others do not accept, and indeed will regard as transgressive and destabilizing, if it is convinced of the rightness of its cause. It will bear the opprobrium that results from imposing the

norm if it believes that, over time, evidence will accumulate that the norm does good work and others will embrace it. The outcast will become a prophet.[34]

The entrepreneurial approach also relies on narratives, but of a different sort from those doing the work of inspiration. It rests on State behaviour and therefore on State acts of self-justification. The entrepreneurial State explains that it not only does not violate international law, but that its actions are those that international law should embrace and perhaps even mandate. The observations of disinterested non-State actors have less of a role, as it is exactly the State's ownership of its choices that provides a pathway for its claim for its choice to become an international norm.

Two examples of this process strike me as compelling. Both involve international economic law rather than humanitarian law. Both involve the United States, which may complicate the story. Perhaps the evolution of the norms in question reflects nothing more than a hegemon's ability to impose its will on the rest of the world. However, a fair reading of these narratives is that the United States anticipated sooner than other States the need for new norms due to changes in the structure of the international economy. After decades of holding out against international resistance, the United States had the satisfaction of seeing other States recognizing that its norm fit a need.[35]

The first norm involved an adjustment of the principle of territorial sovereignty to facilitate effective responses to international cartels. Membership in a cartel requires a firm to forgo sales it otherwise could make and to adhere to the cartel's territorial allotments. The cartels of the interwar period, for example, carved up the world so that industrial giants within a cartel would not compete with another cartel member in the latter's designated territory. Consumers suffered due to lower competition, high prices and an inferior array of products. Because the cartel members who protect another member's monopoly did nothing on the territory of the country where the victimized consumers lived, their (in)action did not meet the traditional standards for prescriptive jurisdiction of the consumers' State. Yet the consumers indisputably suffered economic injury.

The United States responded by asserting a new norm, that prescriptive jurisdiction extended to action or inaction occurring outside a State's territory if the extraterritorial behaviour had a direct, substantial and reasonably foreseeable effect on the well-being of people in the regulating State. On this ground it imposed criminal anti-competition penalties on foreign firms, beginning with a case commenced near the end of the Second World War.[36] Other States fiercely attacked these actions, even imposing criminal penalties on persons who complied with US enforcement measures. By the 1980s, however, most States had come around to the position that international cartels presented an economic threat of common concern and that unilateral acts by injured States did comply

34 See Oona Hathaway and Scott J. Shapiro, "Outcasting: Enforcement in Domestic and International Law", *The Yale Law Journal*, Vol. 121, No. 2, 2011.

35 Paul B. Stephan, "Antibribery Law", in David L. Sloss (ed.), *Is the International Legal Order Unraveling?*, Oxford University Press, New York, 2022, forthcoming.

36 *United States v. Aluminum Co. of America*, 148 F.2d 416, 442-45 (2d Cir. 1945), 12 March 1945.

with customary international law even when the regulated person had not undertaken any positive activity on the territory of the regulating State.[37]

The second story involves a norm against tolerating the payment of bribes to foreign government officials. The United States applies this rule, enforced by criminal and administrative penalties, not only to its own nationals and to people who use US territory to pay bribes, but also to any firm that seeks access to US capital markets. When the United States adopted this legislation in 1977, no other country had such a rule, and many States treated such bribes as ordinary business expenses eligible for tax deductibility. During the 1990s, the United States pushed the members of the Organization for Economic Cooperation and Development (OECD), a club of mostly rich countries, to take similar action. An implicit threat to take more measures against foreign firms if their home countries did not begin to regulate bribery probably helped lead the way to an OECD Convention signed in 1997 that obligates most of the world's rich countries to embrace this norm. In the twenty-first century the United States remains the foremost enforcer of the anti-bribery norm, but other countries have made great strides.[38]

If one wants to look beyond a story about US hegemony in the second half of the twentieth century, the factors that explain both these outlaw-to-prophet stories include a change in thinking about the regulated conduct. Many had seen international cartels and bribery of government officials as matters of parochial concern, rather than as systemic threats to an increasing interconnected world economy. The United States was the first country to see these behaviours as undermining the international integrity of advanced capitalism and thus creating general problems for the world economy. Not only did a growing number of States come to accept the US perspective as legitimate, but they also saw US practice in enforcing the anti-cartel and anti-bribery norms as not skewed toward its own parochial interests (unless you see protecting advanced capitalism as an inherently American parochial concern). US practice, in other words, showed that the norms provided systemic benefits and, in the hands of the State that propounded it, did not lead to substantial impairments of the legitimate interests of other States.

These examples may provide a template for development of the law of armed conflict regarding non-traditional conflicts and cyber-operations as well as international humanitarian law generally. To succeed, the programme requires a significant national actor – a State with skin in the game, as the economists like to say – to announce and comply with rules that constrain its behaviour. The constraint must go further in some clear way than other widely acknowledged

37 American Law Institute, Restatement of the Law Fourth, The Foreign Relations Law of the United States, 2018, § 409.

38 OECD Convention on Combating Bribery of Foreign Public Officials in International Business Transactions, 17 December 1997, Senate Treaty Doc. No. 105-43, 2802 UNTS 225 (entered into force 15 February 1999). See Rachel Brewster, "Enforcing the FCPA: International Resonance and Domestic Strategy", *Virginia Law Review*, Vol. 103, No. 8, 2017, pp. 1646–7; Daniel K. Tarullo, "The Limits of Institutional Design: Implementing the OECD Anti-Bribery Convention", *Virginia Journal of International Law*, Vol. 44, pp. 668–80.

international rules; the actor must otherwise have the capacity to engage in the behaviour that the rule constrains; and the actor must make a plausible case that compliance with the rule means sacrificing some short-term interests. In other words, the actor must be able to convince others that it is willing to pay a cost as the price of the long-term benefits of the rule. The actor moreover must frame the case for the rule in convincing legal terms: this is the point where the inspiration approach and the norm-entrepreneur approach converge. And to be convincing, the case must show that the rule does not provide one-sided benefits to the norm-entrepreneur State, but rather plausibly anticipates systemic benefits that will substantially exceed the costs of compliance.

A few examples may illustrate how particular norm entrepreneurs might address non-traditional armed conflicts and cyber-operations. Consider first the issue of targeting in non-traditional conflicts. States with the capacity to conduct over-the-horizon operations, typically drone strikes, against persons they believe to be implicated in imminent armed attacks have developed non-trivial standards and rules of evidence to constrain military actors in choosing whom to target. The rules aspire to limit the application of armed force only to persons who pose an imminent risk of loss of innocent life and of excluding, or at least limiting as far as possible, collateral damage. The 2015 film *Eye in the Sky* provides a good and, as far as I know, accurate account of what this process looks like.[39] Yet we still have fiascos like the US strike in Kabul on 29 August 2021, to which I referred earlier in this article. The US Air Force Inspector General found that the decisions leading up to this attack did not amount to criminal negligence. The report, the full text of which remains classified, apparently proposes reforms in the rules governing targeting, although we do not know what they are.[40]

For some good to come from this tragedy, it would be helpful if the United States could fix and announce better procedures to guide target assessment for drone strikes. It could then push its allies and friends to do the same. The spread of these practices from States taking part in US-led coalitions, as in Iraq and Syria, to those with whom the United States enjoys friendly relations but which engage in non-conventional conflicts in which the United States does not directly take part, for example Israel, would look very much like the informal creation of a new norm for the law of armed conflict.

Consider next a possible norm that could evolve to constrain a particular type of cyber-operation, namely ransomware. Law aside, nothing precludes a State actor from undertaking an operation with the purpose of extorting payments from the target, but private actors seem at least as willing to profit from these actions. The skills and technology to undertake these attacks may have their origins in the public sector, however, even where the operations are private.

Whether the bandits that run ransomware act on behalf of the State, use capabilities acquired from the State, or rely solely on their own resources and take

39 The film stars my favourite Anglo-Russian actress, Elena Mironova (as it would be in Russian), who her émigré parents named Helen Mironoff and performs under the name Helen Mirren.

40 A. Horton, D. Lamothe and K. Demirjian, above note 12.

no direction from the State, they operate in cyberspace, a place where a number of important States have growing capacities for surveillance and action. With great power comes great responsibility, goes the saying.[41] Perhaps the time has come to develop standards of due diligence applicable to States with significant surveillance capabilities and whose nationals engage in criminal ransomware operations. In June 2021 the White House and the Kremlin established an Experts Group to consider this issue, although its work remains largely protected from public scrutiny.[42]

Much more needs to be done to develop rules of the road for State cyber-operations. I focus on this example only because it draws on well-developed principles of international law, namely those applicable to State responsibility, yet arises in a technologically dynamic environment with unique as well as constantly changing factual predicates. Perhaps, with trial and error as well as implicit agreements rather than formal statements, the cyber great powers can devise among themselves workable standards implementing an obligation on the part of States to suppress internationally harmful cyber-actions undertaken in places or by people within their jurisdiction.

Conclusion

The main difference between the inspirational and norm-entrepreneur approaches to the development of new rules for international humanitarian law pertains to the kinds of explanations made for the rule and the relative importance of published texts and of the contributions of non-State actors, including prominent jurists. I say "relative" advisedly, because the two approaches can complement each other and both undoubtedly are indispensable. However inspirational a proposal may be, it does little work until States consider and embrace it. Actual practice might matter more than formalities in determining whether the proposal engages and moves the international community. At the same time, the process of propounding and applying new norms gains traction and coherence to the extent that publicists explain, criticize and justify the observed practices.

The general point is that, in a period of conflict in and transformation of international relations, States need to find new ways of discovering points of common interest and signalling willingness to conform to particular norms. This may mean developing rules with which States will comply while maintaining plausible deniability that their compliance represents a broader commitment to cooperation or any indication of the normative pull of the rule of law. As international lawyers, we may wish it were otherwise, but the broader purpose of ameliorating the cruelty and inhumanity of armed conflict may require this. To use my last cliché, half a loaf is better than none.

41 See also Luke 12:48: "To whomever much is given, of him will much be required; and to whom much was entrusted, of him more will be asked."

42 The White House, "Fact Sheet: Ongoing Public U.S. Efforts to Counter Ransomware", 13 October 2021, available at: https://www.whitehouse.gov/briefing-room/statements-releases/2021/10/13/fact-sheet-ongoing-public-u-s-efforts-to-counter-ransomware/.