Hybrid CoE Paper 19

Legal power play in cyberspace: Authoritarian and democratic perspectives and the role of international law

Hybrid CoE

Peter B.M.J. Pijpers – February 2024

Hybrid CoE Papers cover work in progress: they develop and share ideas on Hybrid CoE's ongoing research/workstrand themes or analyze actors, events or concepts that are relevant from the point of view of hybrid threats. They cover a wide range of topics related to the constantly evolving security environment.

The European Centre of Excellence for Countering Hybrid Threats
tel. +358 400 253800 www.hybridcoe.fi

ISBN 978–952–7472–92–7 (web)
ISBN 978–952–7472–93–4 (print)
ISSN 2670–2053 (web)
ISSN 2814–7227 (print)

February 2024

Cover photo: Chor muang / Shutterstock.com

Hybrid CoE's mission is to strengthen its Participating States' security by providing expertise and training for countering hybrid threats, and by enhancing EU-NATO cooperation in this respect. The Centre is an autonomous hub for practitioners and experts, located in Helsinki, Finland.

Contents

Summary

The emergence of cyberspace has raised questions about the application of international law, potentially requiring the reinterpretation of existing rules and the need for additional conventions. While this legal reassessment may vary from state to state, there are blocs of like-minded states – authoritarian and democratic – that take opposing positions during consultations at the United Nations. Although these consultations are meant to be legal sessions discussing content, the positions of states often reflect their (geo)political perspectives and vital interests. Conflicting legal opinions of (blocs of) states regarding the application of international law to cyberspace should therefore not only be assessed in the context of legal interpretations, but also understood as the deliberate deployment of legal power play by states as an instrument of power to protect and advance their vital interests.

Introduction

The first laws of war, dating back to the Lieber Code,[1] were drafted when air technology was not yet sufficiently advanced to be used as an instrument of war.[2] As it developed, discussions commenced on how to interpret existing legislation to accommodate the new development, and whether new conventions were required.[3] A similar process occurred after the introduction of nuclear weapons.[4] In both cases, the existing legal framework remained, but the law had to be interpreted to take account of the latest innovations, and hence additional refinements and conventions were sometimes required.

The emergence of cyberspace again raised the question of whether existing international law covers this new technology.[5] The United Kingdom's (UK) Attorney General, Jeremy Wright, hit the nail on the head in 2018 by stating that 'One of the biggest challenges for international law is ensuring it keeps pace as the world changes. International law must remain relevant to the challenges of modern conflicts if it is to be respected, and as a result, play its critical role in ensuring certainty, peace and stability in the international order. If it is seen as irrelevant, it will be ignored and that makes the world less safe'.[6] Barnsby similarly identifies a gap between the 'accelerated pace of change in cyberspace' versus the 'glacial speed at which conventional law develops'[7] – a challenge also applicable to new technologies such as drones, human enhancement, or AI.[8]

Cyberspace is defined in this paper as a human-made domain encompassing a physical layer of hardware (computers, cables and routers), but first and foremost the virtual dimension: that is, the logical layer of software and data, and the virtual personal layer entailing our online representations (LinkedIn or WhatsApp accounts). Activities that can be executed in cyberspace entail digital espionage,[9] extracting data confined in virtual repositories; digital undermining or operations subverting cyberspace itself (often referred to as cyberattacks)

1 Richard R. Baxter, "The First Modern Codification of the Law of War – Francis Lieber and General Orders No. 100 – (II)," *International Review of the Red Cross* 3, no. 25 (1963): 171–89.
2 Ian Henderson, "Manual on International Law Applicable to Air and Missile Warfare : A Review," *Military Law and the Law of War Review* 49, no. 1/2 (2010).
3 Yoram Dinstein, "Air and Missile Warfare Under International Humanitarian Law," *Military Law and the Law of War Review* 52, no. 1 (2013): 81–92.
4 Legality of the Threat or Use of Nuclear Weapons – Advisory Opinion of 8 July 1996, ICJ Reports (1996).
5 See e.g. William H. Boothby, "Where Do Cyber Hostilities Fit in the International Law Maze?," in *New Technologies and the Law of Armed Conflict*, ed. Hitoshu Nasu and Robert McLaughlin (Springer International Publishing, 2014).
6 Jeremy Wright, "Cyber and International Law in the 21st Century," Chatham House, 2018.
7 Robert E. Barnsby, Shane R. Reeves, "Give Them an Inch, They'll Take a Terabyte: How States May Interpret Tallinn Manual 2.0's International Human Rights Chapter," 95 *Texas Legal Review* (2017). p. 1529.
8 Heather A. Harrison Dinniss and Jann K. Kleffner, "Soldier 2.0: Military Human Enhancement and International Law," *Dehumanization of Warfare: Legal Implications of New Weapon Technologies* 92 (2017): 163–205; Gary Corn, "Cyber Operations and the Imperfect Art of 'Translating' the Law of War to New Technologies," *Articles of War*, 2020.
9 Russell Buchan and Inaki Navarrete, "Cyber Espionage and International Law," in *Research Handbook on International Law and Cyberspace*, ed. Nicholas Tsagourias and Russell Buchan, 2nd ed. (Edward Elgar, 2021), 231–52.

with binary code, in order to modify or manipulate data, and to degrade or destroy the ICT (information and communication technology) infrastructure, resulting in (virtual and physical) effects *in* cyberspace; and finally, digital influence operations that use cyberspace as a vector,[10] and target the cognitive dimension.[11]

Does the advent of cyberspace, and the activities that stem from it, necessitate a new treaty, or will existing law suffice? And if existing international law applies to cyberspace, how should it be interpreted? While variations in interpretations in legal opinions (even among kin-like states within the European Union (EU)) are numerous, diverging views are most prominent between countries such as China,[12] Iran, and the Russian Federation (Russia) on the one hand, and "Western" (North America, Australia, EU) countries on the other.[13] Both sides agree that legal lacunas and differences in interpretation exist regarding the application of international law to cyberspace, but their views on how to fill them differ – ranging from drafting new conventions, establishing (new) voluntary non-binding cyber norms, to affirming existing norms.[14] The blocs, authoritarian states versus Western democracies,[15] also clash during international legal consultations at the United Nations (UN),[16] either in the UN Group of Governmental Experts (UN GGE)[17] or the Open-Ended Working Group (OEWG).[18] While the consultations should address legal issues related to standards of sovereignty, *jus ad bellum* and *jus in bello* applicable to cyberspace, the process often reflects the political rather than the legal positions of states.[19] Unfortunately, the armed

10 Christopher Whyte and Brian Mazanec, *Understanding Cyber Warfare: Politics, Policy and Strategy*, (Abingdon: Routledge, 2019). pp. 100–101.

11 Maxime Lebrun, "Anticipating Cognitive Intrusions: Framing the Phenomenon," Hybrid CoE, July (2023).

12 François Delerue and Fan Yang, "Navigating Sino-European Approaches to the Application of International Law in Cyberspace," *Report on the Second Meeting of the Sino-European Expert Working Group on the Application of International Law in Cyberspace* (Geneva, 2023).

13 Maxime Lebrun, "Anticipating Cognitive Intrusions: Framing the Phenomenon." pp. 4–6; Zhixiong Huang and Kubo Mačák, "Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches," *Chinese Journal of International Law* 16, no. 2 (2017): 271–310. pp. 275–278.

14 Mischa Hansel, "Great Power Narratives on the Challenges of Cyber Norm Building," *Policy Design and Practice*, 2023, 1–16. (ahead-of-print version) p.6. Section 4.2.

15 Dennis Broeders, Liisi Adamson, and Rogier Creemers, "A Coalition of the Unwilling ?", *The Hague Program for Cyber Norms*, 2019. Tom Ginsburg, "Authoritarian International Law?," *American Journal of International Law* 114, no. 2 (2020): 221–60; Martha Finnemore and Duncan B. Hollis, "Constructing Norms for Global Cybersecurity," *American Journal of International Law* 110, no. 3 (2016): 425–79. pp. 436–438.

16 Eneken Tikk and Mika Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy," Cyber Policy Institute, 2017; François Delerue, Frédérick Douzet, and Aude Gery, "The Geopolitical Representation of International Law in the International Negotiations on the Security and Stability of Cyberspace," EU Cyber Direct, 2020. pp. 17–24.

17 United Nations GGE 2021 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A 76/135," no. May (2021).

18 United Nations General Assembly, "Final Substantive Report," Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.

19 Taylor Grossman, "Norms vs. Realities: Cyber at the UN," *CSS Analyses in Security Policy*, no. 313 (2022); Hansel, "Great Power Narratives on the Challenges of Cyber Norm Building." pp. 4–8.

conflict that broke out, or rather intensified,[20] after the Russian invasion of Ukraine on 24 February 2022 does not expedite the process of legal alignment.[21]

The purpose of this Hybrid CoE Paper is to assess what the diverging approaches to international law, applicable to cyberspace, mean in terms of hybrid threats and countering them in the Euro-Atlantic context. The key question in the paper is how and why authoritarian and democratic states differ in their interpretation of the application of international law to cyberspace.[22] Given that these are not monolithic blocs,[23] the paper does not turn a blind eye to the differences between democratic states with respect to the application of international law.

To analyze this, the paper will first briefly address the legal debate on the application of international law to cyberspace, before analyzing how the legal positions of authoritarian and democratic states differ, and subsequently why these states have diverging perspectives. The paper concludes with some recommendations for the EU and NATO and their member states.

20 Michael N. Schmitt, "Grey Zones in the International Law of Cyberspace," *The Yale Journal of International Law* 42, no. 2 (2017): 1–21. pp. 1–2.

21 David Miliband, "The World Beyond Ukraine: The Survival of the West and the Demands of the Rest," *Foreign Affairs* 102, no. 3 (2023).

22 Authoritarian and democratic are not defined since the division is not binary. A categorization can nonetheless be made based on the access to political rights and civil liberties, referring to the annual *Freedom in the World* report (https://freedomhouse.org/countries/freedom-world/scores).

23 Delerue, Douzet, and Gery, "The Geopolitical Representation of International Law in the International Negotiations on the Security and Stability of Cyberspace."

Debates on international law in cyberspace

The main issue in the debate on international law in cyberspace is not whether international law applies to cyberspace, but rather how it should be interpreted in light of the characteristics of cyberspace, whether legal lacunas exist and, subsequently, whether the remaining ambiguity justifies new treaties.

The debate is ongoing in the academic realm.[24] While scholars have identified legal gaps, they are divided on how to tackle them. Most black-letter lawyers that adhere to existing law will argue that the current body of law suffices to absorb new developments, while others will argue that new treaties are needed.[25] Hollis is doubtful whether existing international law is suited to regulating the effects on the cognitive dimension, and pleads for new rules for cyberspace.[26] Some scholars highlight the difficulties attached to drafting a treaty. Tsagourias argues that ideally new legislation should be considered, but does not consider this a viable option.[27] Schmitt likewise concludes that 'the prospects for *new* laws applicable to cyberspace are slim'.[28]

The debate is also noticeable among states, which are the key actors and legislators when it comes to international law. Initially, there was uncertainty about the application of international law to cyberspace since many states stayed silent on the matter.[29] The consultations among states on cyberspace in the UN GGE,[30] encouraged by the Tallinn Manual process,[31] have urged states to put forward their official legal opinions (or *opinio iuris)* on how to interpret international law within cyberspace. Paradoxically enough, the current ambiguity is not caused by the silence of states, but by the differences in *opinio iuris* that have since been

24 Aurel Sari, "International Law and Cyber Operations: Current Trends and Developments," in *CAHDI Committee of Legal Advisors on Public International Law* (Strasbourg: Council of Europe, 2023), 1–8.

25 Irène Couzigou, "Securing Cyber Space: The Obligation of States to Prevent Harmful International Cyber Operations," *International Review of Law, Computers and Technology* 32, no. 1 (2018): 37–57. p. 55; Mette Eilstrup-Sangiovanni, "Why the World Needs an International Cyberwar Convention," *Philosophy and Technology* 31, no. 3 (2018): 379–407.

26 Duncan B. Hollis, "The Influence of War; The War for Influence," *Temple International and Comparative Law Journal* 32, no. 1 (2018): 31–46.this essay explores the concept of an influence operation (IO p. 44).

27 Nicholas Tsagourias, "The Legal Status of Cyberspace," in *Research Handbook on International Law and Cyberspace*, 2015, 13–29. p. 29.

28 Michael N. Schmitt, "Taming the Lawless Void: Tracking the Evolution of International Law," *Texas National Security Review* 3, no. 3 (2020): 32–47. p. 47.

29 And some remain ambiguous, including the United States and Israel, see: Roy Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations," *EJIL*, 2020, 1–9.

30 Grossman, "Norms vs. Realities: Cyber at the UN."

31 Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, (Cambridge University Press, 2013); Michael N. Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, 2nd ed. (Cambridge University Press, 2017).

expressed,[32] inter alia by Germany,[33] the Netherlands,[34] Italy,[35] Canada,[36] and Finland.

International law is not set in stone, and leeway in legal interpretation provides essential room for manoeuvre to accommodate novel circumstances or new technological developments such as cyberspace. However, the diverging interpretations on the applicability of international law to a new phenomenon will also lead to ambiguity or even legal uncertainty.[37]

The first question to be addressed is how do states differ in their interpretation of the application of international law to cyberspace, with an emphasis on the differences between authoritarian and democratic blocs.

32 For an overview of national positions, see: https://cyberlaw.ccdcoe.org/wiki/List_of_articles#National_positions.

33 German Ministry of Foreign Affairs, "On the Applicability of International Law in Cyberspace," 2021.

34 Ministry of Foreign Affairs, "Letter to the President of the House of Representatives on the International Legal Order in Cyberspace – Appendix : International Law in Cyberspace" (2019).

35 Italian Ministry of Foreign Affairs, "Italian Position Paper on 'International Law and Cyber Space'," 2021.

36 Government of Canada, "International Law Applicable in Cyberspace," 2022.

37 Peter B.M.J. Pijpers, "Careful What You Wish For Tackling Legal Uncertainty in Cyberspace," *Nordic Journal of International Law* 92 (2023). pp. 414–418.

The application of international law to cyberspace

International law has always been subject to debate,[38] but the emergence of cyberspace appears to have magnified the differences in interpretations. In this section, three issues will be addressed: first, how do interpretations of international law differ between democratic and authoritarian states; second, authoritarian and democratic states are not monolithic blocs, and hence divergences will also occur within these blocs in the reading of international law; and lastly, do these differences necessitate new regulations and treaties.

Diverging interpretations between democratic and authoritarian blocs of states

Democratic and authoritarian blocs differ in their interpretations of the law. Ambiguity arises due to diverse interpretations related to the notions of due diligence,[39] reserved domain,[40] and notifications for countermeasures, to name but a few, when applied to cyberspace.[41] States also differ in their appreciation of international humanitarian law (IHL),[42] or the laws of war. While democratic states apply them in full, authoritarian states are less clear. They highlight the applicability of the general principles but not the body of the law itself.[43]

The diverging interpretations of the applicability of international law to cyberspace are, however, often epitomised in the discourse on the application of sovereignty in cyberspace. While states in general agree that the use of force in cyberspace – when similar in effect to physical attacks – can be seen as a violation of international law,[44] there is less agreement on how sovereignty should be applied in cyberspace.

Sovereignty in cyberspace can be legally assessed from the perspective of its constraining function (what limits the state's conduct outside its territory), or enabling function (what can be regulated based on sovereign jurisdiction).[45] Democratic states highlight the enabling function. While some aspects are the sole authority of the state, others are dealt with via treaties such as environmental or human rights law. Addressing other states that have signed these treaties, or even disseminating propaganda and public diplomacy towards them, is therefore not unlawful per se.

38 Related to e.g., the lawfulness of collective countermeasures or the threshold to invoke self-defence.

39 United Nations GGE 2021 Report, "Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security – A 76/135." Norm 13(h).

40 Ido Kilovaty, "The International Law of Cyber Intervention," in *Research Handbook on International Law and Cyberspace (2nd Ed)*, 2021, 97–112.

41 See also Schmitt, "Grey Zones in the International Law of Cyberspace." under A–F , pp. 4–19.

42 ICRC, "International Humanitarian Law and Cyber Operations During Armed Conflicts," *International Humanitarian Law and Cyber Operations During Armed Conflicts*, 2022.

43 Zhixiong Huang and Yaohui Ying, "Chinese Approaches to Cyberspace Governance and International Law in Cyberspace," in *Research Handbook on International Law and Cyberspace (2nd Ed)*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2020), 547–63.

44 On the use of force and armed attack, another issue arises. Since China and Russia state that information weapons must be banned, they argue that applying these legal standards to the information space (or cyberspace) would legitimize its use. See: Tikk and Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy." p. 16.

45 Inter-American Juridical Committee, *Improving Transparency: International Law and State Cyber Operations 5th Report*, 2020. p. 52.

Within the authoritarian bloc, Cuba, Iran and Venezuela emphasize the sovereign equality of states in cyberspace,[46] highlighting the constraining function of sovereignty by emphasizing their national jurisdiction over cyberspace. In other words, external interference is highly unwelcome, if not unlawful. China argues that cyberspace sovereignty is a 'natural extension of state sovereignty in cyberspace',[47] that cyberspace is thus governed by domestic laws, and that no distinction is made between virtual and physical elements of cyberspace. This is consistent with Iran's position in arguing that 'the territorial sovereignty and jurisdiction of the states are also extended to all elements of the cyberspace'.[48]

Authoritarian states highlight that sovereignty is not restricted to physical boundaries, but argue that states also have digital sovereignty, namely national control over all ICT aspects within state borders. Western democracies, conversely, take a more open approach in which cyberspace is governed by state and non-state entities based on international law. Some academics have even portrayed cyberspace as a Global Commons (lying outside the jurisdiction of one state).[49]

Different interpretations within the blocs

The diverging interpretations – including on sovereignty – are not limited to democratic versus authoritarian states as a bloc. Even within the blocs, there are differences in the reading of international law.[50]

While most democratic states agree that sovereignty – as a notion of international law – applies to cyberspace, not all are convinced that it is a principle of law *and* a binding legal rule in cyberspace. Some, most prominently the UK,[51] are not persuaded that a specific rule on sovereignty exists for cyber activities beyond a prohibited intervention.[52] The UK is not alone in this respect, as the US and Israel are also reticent about the status of sovereignty as a rule in cyberspace.[53] Although the British *opinio iuris* might seem unfortunate amid the legal ambiguity that already exists regarding the application of international law to cyberspace, the position is nonetheless understandable.

46 United Nations General Assembly, "Compendium of Statements in Explanation of Position on the Final Report (A/AC.290/2021/INF/2)," Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security, 2021.

47 Zhang Xinbao and Xu Ke, "A Study of Cyberspace Sovereignty," *China Legal Science* 4, no. 5 (2016): 33–75. p. 34.

48 Armed Forces of the Islamic Republic of Iran, "Declaration Regarding International Law Applicable to the Cyberspace," *Nour News*, no. July (2020).

49 Milton L. Mueller, "Against Sovereignty in Cyberspace," *International Studies Review* 22, no. 4 (2020): 779–801. pp. 794–798.

50 Peter B.M.J. Pijpers, "Exploiting Cyberspace: International Legal Challenges and the New Tropes, Techniques and Tactics in the Russo-Ukraine War," Hybrid CoE, October (2022).

51 More states are ambiguous about the notion of sovereignty in cyberspace, see e.g., Inter-American Juridical Committee, *Improving Transparency: International Law and State Cyber Operations 5th Report*. Bullet 45, p. 55.

52 Wright, "Cyber and International Law in the 21st Century."

53 Schondorf, "Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations."

After all, sovereignty – which entails territorial integrity and political independence – is often framed as 'territorial' sovereignty,[54] while the virtual dimension of cyberspace is inherently non-territorial.[55] The UK's position might be correct taking territorial integrity into account, but political independence (the other element of sovereignty) does apply to activities in cyberspace, irrespective of territory.[56]

Academics chime in as well: Corn and Taylor state that there are sufficient proscriptions against unlawful uses of force and interventions in international law, but that 'below these thresholds there is insufficient evidence of either state practice or *opinio juris* to support assertions that the principle of sovereignty operates as an independent rule of customary international law that regulates states' actions in cyberspace'.[57]

Even among states that accept sovereignty as a rule and principle, diverse nuances in interpretation exist. A case in point is the interpretation of sovereignty as a rule by France (and Switzerland to some extent), which favour a more purist approach to sovereignty, meaning that every breach of ICT is considered a violation of sovereignty,[58] versus Germany, Canada and the Netherlands arguing that 'activities causing negligible or *de minimis* effects would not constitute a violation of territorial sovereignty'.[59]

Although a growing number of states have provided their legal opinions on the applicability of international law, many of them use generic terms that reiterate existing black-letter law without expounding on how international law applies to cyberspace. The Australian legal opinion 'recognises that activities conducted in cyberspace raise new challenges for the application of international law, including issues of sovereignty'.[60] Estonia argues that the 'violation of sovereignty through cyber means can breach international law, and therefore may give the victim state the right to take measures, including countermeasures. Views on what constitutes a breach of sovereignty in cyberspace differ'.[61]

Among authoritarian states, there are also different nuances in terms of their reading of international law. China argues that 'sovereignty in cyberspace is a legally binding principle under international law'. A violation of 'the principle of sovereignty [constitutes] a wrongful act under

54 See e.g., Sean Watts and Theodore Richard, "Baseline Territorial Sovereignty and Cyberspace," *Lewis and Clark Law Review* 22, no. 3 (2018): 771–840. Or Case Concerning Military and Paramilitary Activities in and against Nicaragua, ICJ Reports (1986). Bullets 213, 251.

55 Przemyslaw Roguski, "Layered Sovereignty: Adjusting Traditional Notions of Sovereignty to a Digital Environment," *International Conference on Cyber Conflict,* CYCON, 2019, 347–59. pp. 358–539.

56 Peter B.M.J. Pijpers, *Influence Operations in Cyberspace and the Applicability of International Law* (Edward Elgar, 2023). pp. 234–238.

57 Corn and Taylor, "Sovereignty in the Age of Cyber" p. 208.

58 Ministère des Armées, "Droit International Appliqué Aux Opérations Dans Le Cyberespace," 2019. pp. 5–10.

59 Government of Canada, "International Law Applicable in Cyberspace" Bullet 17.

60 Australian Government, "Australia's Position on the Application of International Law to State Conduct in Cyberspace (Annex B)," 2020.

61 United Nations General Assembly, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies – A /76/136," no. July (2021). p. 25.

international law'.[62] Russia, on the other hand, 'assumes that (...) the international community has reached consensus on the applicability of the universally accepted principles and norms of international law, (...) to information space'.[63] However, the 'majority of Russia's domestic legal instruments pertaining to cyberspace do not refer to international law',[64] not least since Russia regularly implies that relevant international law is absent.

Reinterpreting existing law or the need for new treaties

Despite variations in *opinio iuris* on how to apply international law to cyberspace, most democratic states will argue that existing law suffices for handling activities in cyberspace – even if the question of how to apply international law is still unresolved – while authoritarian states will not. The growing ambiguity urges the more vocal authoritarian states to call for new treaties on cyberspace to regulate the 'legal vacuum'.[65] Iran argues that 'nothing prevents application of noble principles of the UN Charter in the ICT environment. What is left is a legally binding instrument to fill the legal gaps arising from unique features of ICTs', and calls for a convention that regulates the 'use of ICTs by states and other actors, especially those who have dominance in the cyberspace'.[66] Venezuela argues that new binding norms and principles for responsible state behaviour are required,[67] and Russia similarly calls for 'a specialized universal international legal instrument that would envisage criteria for how the existing norms of international law apply to the use of ICTs'.[68]

Both authoritarian and democratic states acknowledge that differences exist in the interpretation of international law with regard to cyberspace. The way to resolve this varies, which leads to the second question on why authoritarian and democratic states differ in their interpretation of the application of international law to this domain.

62 Ministry of Foreign Affairs of the People's Republic of China, "China's Views on the Application of the Principle of Sovereignty in Cyberspace," *UNODA Documents*, 2021, 1–5.

63 United Nations General Assembly, "Official Compendium of Voluntary National Contributions on the Subject of How International Law Applies to the Use of Information and Communications Technologies – A /76/136." pp. 79–80.

64 Sergey Sayapin, "Russian Approaches to International Law and Cyberspace," in *Research Handbook on International Law and Cyberspace (2nd Ed)*, ed. Nicholas Tsagourias and Russell Buchan (Edward Elgar, 2020), 525–46. pp. 525- 530.

65 Russian Delegation to the OEWG, "Statement by the Representative of the Russian Federation at the Online Discussion of the Second 'Pre-Draft' of the Final Report of the UN Open-Ended Working Group," no. June (2020).

66 Iran Minstry of Foreign Affairs, "Intervention by Delegation of the Islamic Republic of Iran on International Law," (2020).

67 Assembly, "Compendium of Statements in Explanation of Position on the Final Report (A/AC.290/2021/INF/2)." p. 90.

68 OEWG, "Statement by the Representative of the Russian Federation at the Online Discussion of the Second 'Pre-Draft' of the Final Report of the UN Open-Ended Working Group."

Authoritarian versus democratic perspectives on the role of international law

The differences in stances between Western democratic and authoritarian blocs are based in part on legal interpretations, but simultaneously on power politics – by both authoritarian states and Western democracies. This section will discuss three topics: first, the legal approaches of authoritarian versus democratic states; second, their perception of cyberspace; and third, the use of international law as an instrument of power.

Legal approaches to international law

Western democracies foster existing international law. In their opinion, international law has universal applicability and acceptance.[69] Legal consultations via the UN GGE are the default procedure for charting a path on how to fit new technologies into existing legal frameworks. Many authoritarian states may have accepted the UN Charter and the conclusions related to some of the UN consultations (UN GGE & OEWG),[70] but acceptance of this body of law does not entail universal applicability.[71]

The Western tendency to foster the universal applicability and acceptance of international law is referred to by Kello as 'cyber legalism'.[72] Although cyber legalism is a normative approach to reduce conflicts via the application of rules and norms, it can be problematic for numerous reasons. First, it reinforces traditional dichotomies between war and peace, which differs from the current geopolitical grey zone and the hybrid approaches of authoritarian states, including Russia and China.[73] Second, it reaffirms the dominant position of Western democracies, which is not conducive to finding a middle ground for legal alignment.

A similar categorisation is made by Lahmann.[74] On the one hand, there is the idea of confining cyberspace to the territorial jurisdiction of a state. In this Westphalian notion, a state should have sovereignty over cyberspace, which is echoed in Chinese and Russian legal opinions and policy papers.[75] On the other hand, there is a perception that cyberspace is a boundless area that is free for all in theory, but in practice dominated by Western (mainly US) tech firms and is, in effect, a new form of 'cyber imperialism',[76] much to the displeasure of Russia and China.

69 Lucas Kello, "Cyber Legalism: Why It Fails and What to Do," *Journal of Cybersecurity*, 2021. p. 7.
70 The 2017 UN GGE could not reach consensus, see also: Tikk and Kerttunen, "The Alleged Demise of the UN GGE: An Autopsy and Eulogy."
71 In 1945 during the inception of the United Nations, the Republic of China (ROC), not the current Chinese regime (People's Republic of China), represented China. The ROC relocated to current-day Taiwan in 1949.
72 Kello, "Cyber Legalism: Why It Fails and What to Do." pp. 4–5.
73 Robert Dalsjö, Michael Jonsson, and Johan Norberg, "A Brutal Examination: Russian Military Capability in Light of the Ukraine War," *Survival* 64, no. 3 (2022): 7–28.
74 Henning Lahmann, "On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace," *Duke Journal of Comparative & International Law* 32, no. 1 (2021): 61–108.
75 Stanislav Budnitsky and Lianrui Jia, "Branding Internet Sovereignty: Digital Media and the Chinese – Russian Cyberalliance," *European Journal of Cultural Studies* 21, no. 5 (2018): 594–613. pp. 599–601; Shanghai Cooperation Organization, "Agreement on Cooperation in Ensuring International Information Security," no. June (2009).
76 Lahmann, "On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace."

The perception of the inception of cyberspace

The discourse on the application of legal standards in cyberspace cannot be assessed solely in legal terms or approaches. The perception of cyberspace and its integration into society frames how states view and value the application of international law.

In 2009, several members of the Shanghai Cooperation Organisation (SCO) – including China and Russia – drafted the International Code of Conduct for Information Security (ICCIS).[77] This strategy refers to the entire information environment, not just cyberspace, and could therefore be viewed as articulating an alternative worldview[78] on the emergence of cyberspace, competing with the dominant (more technical) Western view. The ICCIS argues, on the one hand, that states should comply with the UN Charter in order to combat criminal and terrorist activities, and to curb 'the dissemination of information that incites terrorism, separatism or extremism or that inflames hatred on ethnic, racial or religious grounds'.[79] On the other hand, the ICCIS aims to 'prevent other States from exploiting their dominant position' in ICT when they seek to undermine other 'States' right to independent control of information and communications technology goods and services, or to threaten their political, economic and social security';[80] no doubt referring to Western actors (especially (from) the US) that have been dominant in the technological development of cyberspace, not only as states but also related to non-state actors, including the (independent) ICANN – the Internet Corporation for Assigned Names and Numbers.[81]

In the authoritarian bloc, states such as China and Russia already had policies and legislation in place for state-led activities in the information environment,[82] and the inception of cyberspace can be viewed as an additional toolbox within an existing framework. These activities are often led by intelligence agencies, and executed in the grey zone between peace and armed conflict. Western democracies, on the other side, welcome cyberspace as a new domain alongside existing ones (land, sea and air), often creating a separate Military Cyber Organisation within their defence forces,[83] inherently dividing peacetime engagements from armed conflict.

The way democratic and authoritarian systems view cyberspace also mirrors their perception of the threats and opportunities that stem from it. From the digital authoritarian perspective, information security threats can undermine political and social stability. Dissenting and anti-governmental views (in the Chinese view, 'the 3 evils': terrorism, secessionism or extremism)[84] must be mitigated,[85] and since cyberspace is now the main vector for disseminating these dissenting political views, the internet and social media are often censored. Internet censorship peaks when regime-related choices

77 Shanghai Cooperation Organization, "Agreement on Cooperation in Ensuring International Information Security." (http://eng.sectsco.org/load/207508/).

78 Ruslan Zaporozhchenko, "The End of 'Putin's Empire?' Ontological Problems of Russian Imperialism in the Context of the War against Ukraine, 2022," *Problems of Post-Communism*, 2023. p. 1; Broeders, Adamson, and Creemers, "A Coalition of the Unwilling ?" pp. 1–4.

79 United Nations General Assembly, "International Code of Conduct for Information Security. Letter from the Permanent Representatives of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan to the United Nations Addressed to the Secretary General," *A/69/723*, no. January (2015).

80 United Nations General Assembly. Bullet 2(5).

81 See: https://www.icann.org; see also: Jon Brookin, "Why ICANN Won't Revoke Russian Internet Domains," *Wired*, 2022. China favours transferring the ICANN tasks to the UN-affiliated ITU.

82 Anne-Marie Brady, "Magic Weapons: China's Political Influence Activities under Xi Jinping," Wilson Center, no. September (2017).

83 Max Smeets, "NATO Members' Organizational Path Towards Conducting Offensive Cyber Operations: A Framework for Analysis," in *Silent Battle*, ed. T Minárik et al. (Tallinn: NATO CCD COE, 2019), 163–78.

84 Enshen Li, "Fighting the 'Three Evils': A Structural Analysis of Counter-Terrorism Legal Architecture in China," *Emory International Law Review* 33, no. August (2019): 311–65.

85 Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *Policy Brief, Democracy and Disorder Series*, 2019, 1–22. pp. 2–6.

need to be made, including during elections.[86] Censorship – using software, big data and algorithms – can also be directed, via cyberspace, against diaspora who express their views outside the state.

International law as an instrument of power

In their study on China, Charon and Jeangène Vilmer argue that China is using international law in a strategic way.[87] For them, it is a 'tool of a non-kinetic war that offers influence over an actor's behaviour to strategic ends'.[88] This use of lawfare is a rhetorical confrontation whereby a specific interpretation of international law favours the advancement of national interests. The Chinese Communist Party 'sees itself as engaged in an ideological rivalry with the West, first of all with the United States',[89] and together with Russia they advocate an alternative to the dominant Western view. In a recent joint statement, China and Russia suggest that – related to the war in Ukraine – the Western world is unilaterally bypassing international law, while China and Russia advocate a multipolar world based on the rule of law and the democratization of international relations; in other words, they propose an alternative to the US-dominated world.[90]

The call for new norms and new treaties substantiates authoritarian lawfare as it does not address content but the process of establishing international law. Western states, conversely, are reluctant to advocate new international conventions for cyberspace, since treaties will codify the possibilities of surveillance and restrictions (under the aegis of cybersecurity), will emphasize the digital sovereignty of states, and will serve to 'legitimise repressive state practices',[91] applying censorship and online surveillance, and hence digital authoritarianism[92] by regimes in China, Russia, or the Middle East.[93]

86 Philipp M. Lutscher et al., "At Home and Abroad: The Use of Denial-of-Service Attacks during Elections in Nondemocratic Regimes," *Journal of Conflict Resolution* 64, no. 2–3 (2020): 373–401. pp. 373–374.

87 See also Chapter 4 of Orde F. Kittrie, *Lawfare: Law as a Weapon of War* (Oxford University Press, 2016).

88 Paul Charon and Jean-Baptiste Jeangène Vilmer, "Chinese Influence Operations: A Machiavellian Moment," 2021. p. 31.

89 Charon and Jeangène Vilmer. p. 55.

90 Chris Devonshire-Ellis, "The Putin-Xi Summit – Their Joint Statement and Analysis," *China Briefing*, no. March (2023).

91 United States Department of State, "Other Disarmament Issues and International Security Segment of Thematic Debate in the First Committee of the Sixty-Seventh Session of the United Nations General Assembly," no. November (2012).

92 Fabian Burkhardt and Mariëlle Wijermars, "Digital Authoritarianism and Russia's War Against Ukraine: How Sanctions-Induced Infrastructural Disruptions Are Reshaping Russia's Repressive Capacities", *SAIS Review of International Affairs* 42, no. 2 (2022): 21–43. pp. 21–23.

93 James Shires, *The Politics of Cybersecurity in the Middle East* (London: C Hurst & Co Publishers Ltd, 2021).

Conclusions

Western and authoritarian states adopt different stances on the application of international law to cyberspace, stemming from their legal approach to international law, their perception of cyberspace, and whether they perceive international law as an instrument of power.

The legal differences between authoritarian and Western states on the application of international law to cyberspace should not be exaggerated. There are certainly differences between the authoritarian and democratic blocs of states, but these are not insurmountable, not least since the blocs are not monolithic entities – diverging legal readings persist even within the groups. Moreover, differences in legal interpretations have existed since the establishment of international law; indeed, diverse readings provide indispensable room for manoeuvre once new techniques or circumstances emerge.

Harder to overcome is the legal power play or the use of assertive lawfare. Both authoritarian and Western states leverage international law to legitimise their perspectives on cyberspace. The call for or warning against new international conventions on cyberspace serve as a strategic instrument in this regard.

The concluding reflections for NATO and EU member states are:

- Democratic states need to realize that the Western democratic perspective on cyberspace is dominant at the moment. This is not necessarily based on Western (legal) power play, but merely due to the fact that the internet was, in effect, created in the US.
- Democratic states must also understand that numerous authoritarian states perceive the UN-based international law as a reflection of Western strategic interests. For authoritarian states, the UN Charter and its corollary treaties are universal in their principles, but not in the interpretation of legal norms.[94]
- The dominance in cyberspace and on international law must not lead to complacency. Western democratic states must not underestimate the legal power play used by (gentle giant) China or Russia, especially related to cyberspace – not even after the apparently unsuccessful Russian cyber actions in Ukraine.
- The fabric of Western democratic states, with the rule of law, civil rights and liberties, political responsibility and accountability at its core, is vulnerable to assertive influence operations by authoritarian states, especially when they use hybrid attacks below the level of force. EU and NATO member states need to invest in UN platforms to communicate with other (authoritarian) states on an equal footing to keep lines of communication open. Ironically, the "authoritarian vs democratic" frame is unfortunate as it is oversimplified and can incite polarisation.
- NATO and the EU should acknowledge that lawfare (for better or worse) is a substantial instrument of state power and, for many states, an integral and synchronized part of their hybrid threat toolbox.
- While respecting EU and NATO mandates and origins, the only way to counter hybrid threats that include a severe legal component is to cooperate, and to complement each other's instruments of power.

94 This stems in part from the notion that the Chinese signatory to the UN Charter was not the current People's Republic regime, but the former Republic of China that fled to Taiwan.

Author

Peter B.M.J. Pijpers, PhD, is an Associate Professor of Cyber Operations at the Netherlands Defence Academy and a researcher at the Amsterdam Centre of International Law (ACIL), University of Amsterdam.

Correspondence address: b.m.j.pijpers@uva.nl.
Orcid ID: https://orcid.org/0000-0001-9863-5618.

Hybrid CoE

The European Centre of Excellence
for Countering Hybrid Threats