German Law Journal (2023), **24**, pp. 508–521
doi:10.1017/glj.2023.27

ARTICLE

Special Issue: International Law and Digitalization

Does Digitalization Reshape the Principle of Non-Intervention?

Lukas Willmer[1, 2]

[1]Humboldt University of Berlin, Berlin, Germany and [2]Berlin Potsdam Research Group "The International Rule of Law – Rise or Decline?", Berlin, Germany
Email: lukas.willmer@kfg-intlaw.de

(Received 10 April 2023; accepted 11 April 2023)

Abstract
While digitalization has led to renewed attention to the principle of non-intervention, not the least by Western states rediscovering the protective dimension of sovereignty, it remains plagued by a certain vagueness. Attempts by academics to fill the gaps lead to starkly different results, ranging from the insertion of democratic values to the inadvertent reinforcement of protectionist tendencies. Overall, digitalization has so far had less of an effect on the principle of non-intervention than its renewed importance may have on the type of international law more generally.

Keywords: Non-intervention; cyberspace; election interferences; regime neutrality

A. Of Moats and Drawbridges

For the utopia of an interconnected, globalized world, where information freely flows across borders and states are massively interdependent, the principle of non-intervention seems like a Westphalian castle with moats and drawbridges in between glitzy, translucent glass towers.

Since the end of the Cold War, a "cosmopolitan paradigm" has supposedly developed that "celebrates the international level as "domesticating" sovereignty and its attendant risks."[1] The expansion of international law, especially human rights law, has diminished the *domaine réservé* and, so goes the argument, with it the scope and importance of the principle of non-intervention. Indeed, Western states, arguably the most ardent supporters of this development, have largely refrained from even mentioning the principle at the UN.[2] Yet the principle of non-intervention is back on the agenda, in particular within the cyber context. Interconnectedness also creates vulnerabilities and Western states especially have realized that open and pluralistic societies may be less resilient against foreign interferences than assumed. Of course, not all states share this utopia of interconnectedness in the first place, and for many non-Western states, the principle of non-intervention has never been off the agenda. Many states have continuously been warier of foreign interferences even before the digital age.

[1]Tom Ginsburg, Democracies and International Law 5 (2021).

[2]This neglect had extended to Western academia, the only more prominent article dealing substantively with the principle appears to be the one by Maziar Jamnejad & Michael Wood, *The Principle of Non-intervention*, 22 Leiden J. Int'l L. 345 (2009).

Does digitalization reshape the principle of non-intervention? This Article will offer some observations. Most importantly, digitalization has led to renewed attention for the principle broadening the scope of state actors that invoke it (B). This renewed attention has, however, not led to further clarity regarding its application (C). Finally, it is worthwhile to note the possible effect of certain academic proposals on the values underlying the principle of non-intervention (D). It will be argued that, at least so far, digitalization has had less of an effect on the principle of non-intervention itself, than the principle's renewed importance may have on the type of international law more generally (E).

B. Renewed Attention: A Broadened Scope of State Actors Invoking Non-intervention

Digitalization has led to renewed attention to the principle of non-intervention and, more importantly, broadened the scope of states invoking it. Basic assumptions about which states are likely to rely on the principle become invalid. It is no longer invoked primarily by comparatively weak (I) or authoritarian states (II).

I. Power Asymmetries

First, the principle of non-intervention has in the past mostly been invoked by weaker states against more powerful states.[3] When it found expression in the Monroe doctrine, it was an attempt by the US, at that point young and relatively weak, to fend off influence from former colonial powers in the Americas.[4] When US foreign policy became more and more dominant in the region, Latin American states embraced the principle to oppose just that.[5] After the decolonization process, newly independent states guarded their hard-won sovereignty.[6] Even in the rare instance in which a Western state alludes to the principle, such as when Germany objected to US sanctions against the North Stream II pipeline as an interference in its internal affairs,[7] it takes place in a situation of clear power asymmetry. Digitalization, at least for now, changes the assumption that a powerful actor has relatively little to fear from weaker adversaries. Cyber weapons are comparatively cheap and easy to acquire compared to conventional capabilities. The US, for example, is not only concerned about Russian and Chinese cyber activities, but also about cyber operations in Iran and North Korea.[8] Germany has warned that "[i]n cyberspace, only limited resources are often needed to cause significant harm."[9] It remains to be seen, though, whether this development will consolidate in the long run or whether more technologically advanced states will eventually be able to adapt and protect themselves against cyber-attacks while states with less cyber capabilities remain vulnerable.

II. The "Authoritarian Stain" of the Principle of Non-intervention

Second, the principle of non-intervention tended to be invoked by more authoritarian states to fend off foreign criticism, or, as they perceive it, foreign interferences. It is especially important but

[3]Stephen D. Krasner, Sovereignty: Organized Hypocrisy 25 (1999).

[4]Hanspeter Neuhold, The Law of International Conflicts: Force, Intervention and Peaceful Dispute Settlement 163 (2015).

[5]Arnulf Becker Lorca, Mestizo International Law: A Global Intellectual History 1842–1933 341–352 (2014).

[6]Neuhold, *supra* note 4, at 165.

[7]German Government Press Release 432, German Government Notes Sanctions Against Nordstream 2 and Turkstream with Regret (Dec. 21, 2019) https://www.bundesregierung.de/breg-de/suche/bundesregierung-nimmt-sanktionen-gegen-nordstream2-und-turkstream-mit-bedauern-zur-kenntnis-1708962 [hereinafter Germany].

[8]Off. of the Dir. of Nat'l Intel., Annual Threat Assessment of the US Intelligence Community 20 (2021).

[9]Germany, *On the Application of International Law in Cyberspace* 1 (2021) https://www.auswaertiges-amt.de/blob/2446304/32e7b2498e10b74fb17204c54665bdf0/on-the-application-of-international-law-in-cyberspace-data.pdf.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

also difficult in this regard to distinguish between political and legal invocations of the principle of non-intervention.[10] For example, the concerted effort by China and a significant number of other states to defend Chinese treatment of Uighurs in Xinjiang as a domestic matter in the Third Committee of the General Assembly extends beyond political rhetoric.[11] Similarly, the increasing enactment of domestic legislation against foreign funding for NGOs backs up a legal claim against political interference through "democracy promotion" that some states consider to be a violation of the principle of non-intervention.[12] The preference by authoritarian states for the principle of non-intervention may explain why China, despite its rise to global power status, continues to embrace the principle as one of the basic pillars of its foreign policy, at least on the rhetorical level.[13] Meanwhile, Western states have rarely invoked the principle of non-intervention in the past, they have largely avoided even mentioning it in the context of the UN. At least for some states, the principle of non-intervention appeared to have an "authoritarian stain".

Effects of digitalization challenge this assumption as well. Western states have stopped avoiding the principle and started to refer to it in the cyber context, although this did take some time. The debate over international law in cyberspace was, at least within the UN, kickstarted by Russia, which in 1998 brought the topic to the UN's agenda.[14] Yet the discussions did not produce any substantial outcomes, primarily due to a lack of interest among Western states in cyber regulation. This attitude changed after the 2007 cyber-attack against Estonia.[15] In 2013, the UN Governmental Group of Experts (GGE) reached a consensus that international law, and in particular the UN Charter, applies to cyberspace.[16] In 2015, the GGE went further and specifically identified, *inter alia*, the principle of non-intervention as being applicable in cyberspace.[17] This consensus has subsequently been confirmed in the 2021 GGE report[18] as well as by an additionally established Open-Ended Working Group (OEWG)[19] and by the General Assembly[20]. All states that have put forward their views on how international law applies in cyberspace engaged, at least to some extent, with the principle of non-intervention. This is not surprising because non-intervention is likely the most obvious norm to regulate violations of sovereignty below the threshold of uses of force. It also became increasingly clear that "cyberwarfare" could not be regulated solely through the prism of Article 2(4) UN Charter.[21] Within statements from Western states, reluctance to rely on the principle of non-intervention because of an "authoritarian stain" was no

[10]*See* Jamnejad & Wood, *supra* note 2, at 347.

[11]U.N. GAOR, 74th Sess., at 12, UN Doc A/C.3/74/SR.37 (Nov.26, 2018).

[12]Heike Krieger, *Populist Governments and International Law*, 30 Eur. J. Int'l L. 971, 991–994 (2019).

[13]*See, e.g.,* The Declaration of the Russian Federation and the People's Republic of China on the Promotion of International Law, U.N. Doc A/70/982, para. 4 (Jul. 8, 2016); *see also* Congyan Cai, The Rise of China and International Law 94 (2019).

[14]G.A. Res 53/70 (Jan. 4, 1999); *see also* Permanent Rep. of the Russian Federation, Letter dated 23 September 1998 from the Permanent Representative of the Russian Federation to the United Nations addressed to the Secretary-General, U.N. Doc A/C.1/53/3 (Sept. 30, 1998).

[15]Liisi Adamson, *International Law and International Cyber Norms: A Continuum?*, *in* Governing Cyberspace: Behavior, Power and Diplomacy 21 (Dennis Broeders & Bibi van den Berg eds., 2020).

[16]Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 19, U.N. Doc A/68/98, (June 24, 2013) [hereinafter GGE Report 2013].

[17]Rep. of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, para. 28(b), U.N. Doc A/70/174 (July 22, 2015) [hereinafte GGE Report 2015].

[18]Rep. of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security, para. 2 (May 28, 2021) https://front.un-arm.org/wp-content/uploads/2021/06/final-report-2019-2021-gge-1-advance-copy.pdf (forthcoming) [hereinafter GGE Report 2021].

[19]Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security – Final Substantive Report, para. 8, U.N. Doc A/AC.290/2021/CRP.2 (Mar. 10, 2021) [hereinafter OEWG Report].

[20]G.A. Res. 75/240 (Dec. 31, 2020); G.A. Res 75/32 (Dec. 7, 2020); G.A. Res 73/266 (Dec. 22, 2018); *see also* G.A. Res 70/237 (Dec. 23, 2015).

[21]*See* Mary Ellen O'Connell, *Cyber Security without Cyber War*, 17 J. Conflict & Sec. L. 187, 199 (2012).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

longer perceivable. On the contrary, Western states provided the most detailed assessments of how the principle of non-intervention applies in cyberspace.[22] Back in 1981, Western states unanimously rejected the General Assembly Declaration on Intervention[23] because they opposed the concept of a "New International Information Order", which, *inter alia,* held the dissemination of false or distorted news as unlawful.[24] Now, under increasing pressure from cyber election interferences and certain forms of destabilization of public discourses more generally, some Western states appear to embrace the idea that certain disinformation campaigns can violate the principle of non-intervention.[25]

C. Regulatory Vagueness: Which Standards of Non-intervention in Cyberspace?

Despite the renewed interest that digitalization has sparked in the principle of non-intervention, its regulatory vagueness persists. States have so far primarily affirmed its applicability to cyberspace without reaching any consensus on how it applies (I). While the proposal by some states to adopt an entirely new cyber treaty has not garnered sufficient support, consensus seems to be more easily reachable with regard to non-binding rules. Those rules may, however, threaten to informalize even accepted international law (II). A fragmentation of regulatory processes at the UN is further complicating the issue (III).

I. Affirming Applicability, not Clarifying the Application

The principle of non-intervention was always plagued by a certain vagueness. In the early 1920s, Winfield remarked that a "reader, after perusing Phillimore's chapter upon intervention, might close the book with the impression that intervention may be anything from a speech of Lord Palmerston's in the House of Commons to the partition of Poland."[26] According to the ICJ's *Nicaragua* judgment, an intervention is prohibited if it bears on matters in which each state

[22]Australian Mission to the United Nations, *Open Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security* (2019) https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/fin-australian-oewg-national-paper-Sept-2019.pdf [hereinafter Australia]; Government of Canada, *International Law Applicable in Cyberspace* (2022) https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a3 [hereinafter Canada]; Kersti Kaljulaid, President, President of the Republic at the opening of CyCon 2019 (2019) [hereinafter Estonia]; French Ministry of Defense, *Droit International Appliqué aux Opérations dans le Cyberespace* (2019), droit-internat-appliqué-aux-opérations-cyberespace-france.pdf (justsecurity.org) [hereinafter France]; Government of Finland, *International Law and Cyberspace* (2020) https://um.fi/documents/35732/0/KyberkannatPDF_EN.pdf/12bbbbde-623b-9f86-b254-07d5af3c6d85?t=1603097522727 [hereinafter Finland]; Germany, *supra* note 7; Roy Schondorf, *Israel's Perspective on Key Legal and Practical Issues Concerning the Application of International Law to Cyber Operations*, EJIL: TALK!: BLOG OF THE EUR. J. OF INT'L L. (Dec. 8, 2020) https://www.ejiltalk.org/israels-perspective-on-key-legal-and-practical-issues-concerning-the-application-of-international-law-to-cyber-operations/; Appendix to Letter of 5 July 2019 from the Minister of Foreign Affairs to the President of the House of Representatives on the international legal order in cyberspace (July 1, 2019) https://www.government.nl/ministries/ministry-of-foreign-affairs/documents/parliamentary-documents/2019/09/26/letter-to-the-parliament-on-the-international-legal-order-in-cyberspace [hereinafter Netherlands]; New Zealand Foreign Affairs an*The Application of International Law to State Activity in Cyberspace*, NEW ZEALAND (2020) https://www.mfat.govt.nz/assets/Peace-Rights-and-Security/International-security/International-Cyber-statement.pdf [hereinafter New Zealand]; United Kingdom Foreign, Commonwealth and Development Office, *Application of international law to states' conduct in cyberspace: UK statement* (2021) https://www.gov.uk/government/publications/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement [hereinafter United Kingdom]; Brian J. Egan, Legal Advisor, Remarks on International Law and Stability in Cyberspace (Nov. 10, 2016) https://2009-2017.state.gov/s/l/releases/remarks/264303.htm [hereinafter United States].

[23]G.A. Res. A/RES/36/103, Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, (1981). Finland and Greece abstained.

[24]*Id.* at 2. III. lit. d.

[25]*See, e.g.,* New Zealand, *supra* note 22, para. 10; Germany *supra* note 7, at 5; *see also* France, *supra* note 22, at 7.

[26]Percy Henry Winfield, *The History of Intervention in International Law*, 3 BRIT. YEARBOOK INT'L L. 130 (1922-23).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

is, by the principle of state sovereignty, permitted to decide freely while employing methods of coercion.[27] Yet, what exactly constitutes coercion has always remained unclear, with Western states tending to propose a rather narrow understanding while many non-Western states advocate including, for example, unilateral economic sanctions as a form of economic coercion as well.[28]

The debates in the GGE and OEWG have not shed much further light on this topic. While many states and several of the final reports have affirmed the applicability of the principle of non-intervention to cyberspace, they did not provide much guidance as to its interpretation. For example, the Chinese submission to the OEWG is limited to the statement that the "principles enshrined in the UN Charter, including sovereign equality, refraining from the use of force, settlement of disputes by peaceful means and non-intervention in the internal affairs of other states, apply in cyberspace."[29] Japan submits that "[w]ith respect to the principle of non-intervention, cyber operations may constitute unlawful intervention when requirements including the element of coercion, which are clarified in the Nicaragua judgement (1986), are met."[30]

Statements by states that did go into more detail almost all came from Western states.[31] Within those statements, different standards of coercion become particularly apparent regarding cyber election interferences. Some states appear to adhere to a narrower interpretation. When giving specific examples, these states only refer to interferences manipulating the actual vote tally or, at least partly, preventing the holding of the election at all as a form of coercive behavior.[32] Although the UK, in more elaborate remarks on non-intervention, stated that it considers coercion to be broader than forcing a state into specific conduct also encompassing acts that "depriv[e] a State of its freedom of control," it still only gave interferences with the technical election infrastructure as examples.[33] Other states seem to consider disinformation campaigns at least as possibly being coercive.[34] Germany, for example, is more elaborate in its position, considering online disinformation campaigns as coercive if they "deliberately incite violent political upheaval [. . .] significantly impeding the orderly conduct of an election" as they "may be comparable in scale and effect to the support of insurgents."[35] The broadest—and most vague—interpretation is offered by France which suggests that a digital "interference which causes or may cause harm to France's political, economic, social and cultural system, may constitute a violation of the principle of non-intervention."[36] Thus, there is no consensus whether activities such as the alleged Russian interferences in the 2016 US Presidential elections, which did not affect the technical election infrastructure but rather targeted the public discourse, is prohibited by the principle of non-intervention. It is possible, that interfering with the technical election infrastructure constitutes the *de minimis*-threshold for those states that provide it as a sole example. It may also be the

[27]Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. Rep. 14, para. 190 (June 27, 1986).

[28]*See, e.g.*, G.A. Res 74/200 (Jan. 13, 2020).

[29]OEWG, *China's Submissions to the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security 6* (2019) https://unoda-web.s3.amazonaws.com/wp-content/uploads/2019/09/china-submissions-oewg-en.pdf; *see also* Colombia, Informe Recolución A/RES/75/32 16 (2021) https://front.un-arm.org/wp-content/uploads/2022/03/colombia-ict-security-2021.pdf.

[30]OEWG, *Basic Position of the Government of Japan on International Law Applicable to Cyber Operations 2* (May 28, 2021) https://www.mofa.go.jp/files/100200935.pdf [hereinafter Japan].

[31]*See* Australia, *supra* note 22; Canada, *supra* note 22; Estonia, *supra* note 22; France, *supra* note 22; Finland, *supra* note 22; Germany, *supra* note 22; Israel, *supra* note 22; The Netherlands, *supra* note 22; New Zealand, *supra* note 22; United Kingdom, *supra* note 22; United States, *supra* note 22.

[32]Australia, *supra* note 22, at 8; Canada, *supra* note 22, para. 24; Schondorf, *supra* note 22; United Kingdom, *supra* note 22, para. 9; United States, *supra* note 22.

[33]Suella Braverman, Sec'y of State for the Home Dept. Address Concerning International Law in Future Frontiers (2022) https://www.gov.uk/government/speeches/international-law-in-future-frontiers.

[34]Netherlands, *supra* note 22, at 3; New Zealand, *supra* note 22, para. 10.

[35]Germany, *supra* note 7, at 5.

[36]France, *supra* note 22, at 7.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

case, that these states remain strategically silent regarding lower-level interferences for the time being.[37] In any event, the debate is an almost entirely intra-Western debate. Even if this debate eventually produces a consensus position within Western states, it would not be sufficiently widespread and representative to further develop custom. The only exception is a detailed statement released by the General Staff of the Iranian Armed Forces, which mentions "[m]easures like cyber manipulation of elections or engineering the public opinions on the eve of the elections [as] examples of gross intervention."[38] The large majority of states have opted not to provide their opinion at all, despite manifold invitation to do so.[39] There are various reasons for this. An important factor is certainly a lack of capacity.[40] For many states, foreign election interferences may also not be the most pressing concern. And those states that, in the long term, envision the adoption of an entirely new cyber treaty may not provide their substantive views as their central argument is that existing international law is not sufficiently precise in regulating cyberspace. Developing custom would close the gap which is supposed to be filled by a treaty.

Thus, the GGE and OEWG reports accurately reflect the current consensus: The principle of non-intervention applies in cyberspace—but how it applies is unclear. The approach offered by Germany, namely that a cyber operation is coercive if its scale and effect are comparable to an operation in the non-cyber context appears convincing at first, as it purports to simply transpose the existing principle to the cyber context. A similar test is also advanced by many states regarding the use of force, known as "kinetic effect".[41] But how the principle of non-intervention applies in the non-cyber context, specifically where the threshold of coercion lies, is equally unclear. The last attempt to further clarify the content of the principle dates back to 1981 and was not universally accepted.[42] Germany references the support for insurgents as an example. This has indeed been considered coercive by the ICJ in *Nicaragua*, but as a "particularly obvious" form of coercion,[43] not as *de minimis*-threshold. Yet it is precisely the question of where this threshold lies that makes the application of the principle of non-intervention so difficult in practice. Despite renewed attention, the principle of non-intervention remains vague. States thereby risk retaining a principle that will be often invoked, but sufficient consensus on whether it has actually been breached will be seldomly reached.

Circumventing the difficult debate about coercion, some states,[44] as well as scholars,[45] appear to have shifted the focus to a different norm. The discussion whether sovereignty itself is merely a principle from which specific rules are drawn or a rule itself seems to be motivated, at least in part, by uncertainties in which cyber operations cross the coercion threshold.[46] But, being ill-defined

[37]This at least used to be the UK position, *see* Doug Wilson, Introductory Remarks on the Promise and Limits of Cyber Power in International Law (2020); *but see* United Kingdom, *supra* note 22*; see also* Sue Robertson, Introductory Remarks on the Promise and Limits of Cyber Power in International Law (2020).

[38]Press Release, General Staff of Iranian Armed Forces Warns of Tough Reaction to Any Cyber Threat (2020) https://nournews.ir/En/News/53144/General-Staff-of-Iranian-Armed-Forces-Warns-of-Tough-Reaction-to-Any-Cyber-Threat [hereinafter Iran].

[39]*See, e.g.*, GGE, G.A. Res. A/RES/73/266, para. 2 (Dec. 22, 2018); OEWG, G.A. Res. A/RES/73/27, para. 4 (Dec. 5, 2018); Duncan B. Hollis, Presentation for the Inter-American Judicial Committee, Improving Transparency: International Law and State Cyber Operations (Aug. 7, 2020).

[40]Hollis, *supra* note 39, at 6.

[41]*See, e.g.*, Iran, *supra* note 38, at art IV; Netherlands, *supra* note 22, at 3; New Zealand, *supra* note 22, para. 7; United States, *supra* note 22.

[42]Declaration on the Inadmissibility of Intervention and Interference in the Internal Affairs of States, *supra* note 23.

[43]Nicar. v. U.S., 1986 I.C.J. para. 205.

[44]France, *supra* note 22, at 7; Japan, *supra* note 30, at 3; Netherlands, *supra* note 22, at 2; Germany, *supra* note 7, at 3; Hollis, *supra* note 39, at 30.

[45]Michael N. Schmitt, Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 17 (2017).

[46]Henning Lahmann, *On the Politics and Ideologies of the Sovereignty Discourse in Cyberspace,* 32 Duke J. Compar. & Int'l L. 61, 90 (2021).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

and at least as politically charged as the principle of non-intervention, one might wonder whether this simply leads to the replacement of one empty container with another one.

II. Calls for a Cyber Treaty vs. Trends Towards Informalization

A different response to the lack of clarity of the principle of non-intervention—and international law in cyberspace more generally—are calls to adopt a cyber treaty.[47] It is claimed that from cyberspace emerge "unique problems without ready solutions in the existing legal framework."[48] The application of general international law such as the principle of non-intervention is only a first step, on top of which a "framework charter for cyberspace activities" should be drafted.[49] Yet, Western states in particular reject the idea of a treaty. Since it has already been confirmed that international law as a whole applies to cyberspace, it is feared that a convention might lead to picking and choosing of certain rules[50] and that "it opens the gate for an *argumentum e contrario* for putting in question the applicability and legally binding character of customary international law, general principles of law and treaty obligations with regard to ICTs."[51] In the 2021 Report of the OEWG, all references to a new binding framework that still existed in the Zero Draft[52] as well as the Pre-Draft[53] have vanished. Yet the 2021 GGE report "notes the possibility of future elaboration of additional binding obligations, if appropriate."[54] Given this fundamental impasse with some states advocating to further develop existing custom and thus resisting a new treaty, and other states favoring a treaty and thus not providing their views on how to develop existing custom, it is maybe not surprising that the current consensus at the UN does not extend far beyond confirming the application of international law to cyberspace. How specific norms and principles and in particular the principle of non-intervention apply in concrete circumstances remains, at least for now, uncertain.

What can be achieved more easily seems to be a consensus on voluntary, non-binding norms or responsible state behavior. The 2021 GGE report, for example, deals with international law on one and a half pages while elaborating on eight and a half pages on non-binding norms.[55] While it is often argued that non-binding norms may eventually become custom,[56] some may advance adoption as a non-binding norm as an argument for the opposite. One example is the UK's 2021 statement on the application of international law to cyberspace. According to the non-binding norm 13(c) adopted by the GGE in 2015, states "should not knowingly allow their territory to be used for internationally wrongful acts using information and telecommunications technology."[57] The UK stresses that "the fact that States have referred to this as a non-binding norm indicates that there is not yet state practice sufficient to establish a specific customary international law rule of 'due diligence' applicable to activities in cyberspace."[58] Although norm 13(c) reflects what the ICJ

[47]*See* submissions by China, Cuba, Egypt, India, Malaysia, Russia at the OEWG, United Nations, OEWG, *5th Meeting of the First Substantive Session* (Sept. 11, 2019) https://media.un.org/asset/k1f/k1fbpdsxqt; *see also* China, *supra* note 29, para. 6.

[48]Ma Xinmin, *What Kind of Internet Order Do We Need?*, 14 CHINESE J. INT'L L. 399, 401 (2015).The author was, at the time of writing, a member of the Department of Treaty and Law at the Chinese Ministry of Foreign Affairs.

[49]*Id.* at 400–401.

[50]United Nations, *supra* note 47, at 1:04:00 hrs.

[51]OEWG, *Comments on the Pre-Draft Report of the Open Ended Working Group – ICT 2* (Mar. 31, 2020) https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf [hereinafter Austria].

[52]OEWG, *Draft Substantive Report*, UN Doc A/AC.290/2021/L.2, para. 32 (Jan. 19, 2021).

[53]OEWG, *Initial "Pre-Draft" of the Report of the OEWG on Developments in the Field of Information and Telecommunications in the Context of International Security*, para. 27 (Apr. 27, 2020).

[54]GGE Report 2021, *supra* note 18, at 16.

[55]*Id.* paras. 15–73.

[56]Kubo Mačák, *From Cyber Norms to Cyber Rules: Re-engaging States as Law-makers*, 30 LEIDEN J. INT'L L. 877, 892-893 (2017); Michael N. Schmitt, *The Sixth United Nations GGE and International Law in Cyberspace,* JUST SEC. (2021), https://www.justsecurity.org/76864/the-sixth-united-nations-gge-and-international-law-in-cyberspace/.

[57]GGE Report 2015, *supra* note 17, para. 13 (c).

[58]United Kingdom, *supra* note 22, para. 12.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

has accepted as law in *Corfu Channel*,[59] it is indeed disputed whether and how due diligence applies in cyberspace.[60] The merits of this debate are beyond the scope of this paper, but the example illustrates that the formulation of non-binding norms within an area that is already —partly—regulated by international law may be a double-edged sword.

Instead, this approach risks informalizing even accepted rules of international law. The 2013 GGE Report combined recommendations on norms, rules, and principles of responsible behavior by states into one category.[61] The 2015 and 2021 GGE Reports clearly distinguish again between binding and non-binding norms.[62] But some of the norms that the GGE lists within its report as non-binding closely replicate existing international obligations. This is most obvious in the case of norm 13(f) adopted by the GGE in its 2015 report according to which a "State should not conduct or knowingly support ICT activity *contrary to its obligations under international law* that intentionally damages critical infrastructure [. . .]"[63] Norm 13(f) thus establishes a non-binding, voluntary norm to obey the law. The problem is not limited to the GGE outcome. The non-binding SCO Draft Code of Conduct includes a pledge "[n]ot to use information and communications technologies and information and communications networks to interfere in the internal affairs of other states or with the aim of undermining their political, economic and social stability."[64] Compliance with the principle of non-intervention is phrased here as a voluntary choice.

Both developments would likely cause spill-over effects in the non-cyber context. Provisions made in a cyber treaty may very well affect what is deemed as acceptable "analog" interference. Increasing informalization could further erode the principle of non-intervention in general.

III. Fragmentation of Regulatory Processes: from GGE and OEWG to PoA?

What has further complicated the issue is the fragmentation of the processes in which cyber issues are discussed at the UN. The primary venues were several GGEs that had been convened, with interruptions, since 2004.[65] While their outcomes, especially those in 2013 and 2015, have been lauded, the groups have also been criticized for being non-transparent, exclusive, and unable to engage in a multi-stakeholder dialogue.[66] The GGEs are only open to a limited number of governmental experts appointed by the Secretary-General.[67] It was, at least by some states, perceived to be dominated by Western experts and ended up deadlocked in 2017.[68] Thus, in 2019 Russia initiated the OEWG, which is open to all member states and was presented as an attempt to make the process "more democratic, inclusive and transparent."[69] It was also perceived as a potential forum to negotiate a cyber treaty,[70] although in the end, it was the GGE report where a reference to the

[59]Corfu Channel Case (U.K. v. Alb.), Merits, Judgment, 1949 I.C.J. 4, 22 (Apr. 9).

[60]*See,* e.g., Eric Talbot Jensen, *Due Diligence in Cyber Activities*, *in* Due Diligence in the International Legal Order (Heike Krieger, Anne Peters & Leonhard Kreuzer eds., 2020).

[61]GGE Report 2013, *supra* note 16, at 8.

[62]GGE Report 2015, *supra* note 17, at 7, 12; GGE Report 2021, *supra* note 18, at 4, 13.

[63]GGE Report 2015, *supra* note 17, at 7. This is also reaffirmed in OEWG Report 2021, *supra* note 18, para. 31.

[64]China, Kazakhstan, Kyrgyzstan, Russian Federation, Tajikistan, Uzbekistan, International code of conduct for information security, Permanent Representative of China, Letter dated 9 January 2015 from the Permanent Representative of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan, and Uzbekistan to the United Nations addressed to the Secretary-General, para. 2(3), U.N. Doc A/69/723 (Jan. 13, 2015).

[65]G.A. Res 60/45 (Jan. 6, 2006).

[66]François Delerue, *From Multilateral to Multistakeholder? New Developments in UN Processes on Cybersecurity,* Council on Foreign Relations Blog (2020), https://www.cfr.org/blog/multilateral-multistakeholder-new-developments-un-processes-cybersecurity.

[67]G.A. Res 60/45 para. 4 (Jan. 6, 2006).

[68]Xymena Kurowska, *What Does Russia Want in Cyber Diplomacy? A Primer*, *in* Governing Cyberspace: Behavior, Power and Diplomacy 94-95 (Dennis Broeders & Bibi van den Berg eds., 2020).

[69]G.A. Res 73/27 para. 5 (Dec. 11, 2018).

[70]Kurowska, *supra* note 68, at 87.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

development of additional norms was retained while it disappeared in the OEWG report.[71] To reunite the dual-tracked process, a diverse group of states led by Egypt and France have suggested continuing the debate at a permanent "Programme of Action for advancing responsible State behavior in cyberspace" (PoA).[72] According to the proposal, the PoA would create a framework and political commitment based on the GGE/OEWG *acquis,* and have regular working-level meetings focused on implementation as well as review conferences.[73] It would also step up capacity building and create an institutional dialogue with other stakeholders.[74] Establishing a PoA could, first of all, offer a way out of the geostrategic rivalries that are associated with the GGE/OEWG. Another advantage that has been noted is that it would allow for dissociating different subjects.[75] But judging from the outcome of the GGE/OEWG so far, there is at least the risk that international law questions, which have so far been difficult to answer, would be sidelined. For example, while the PoA on small arms and light weapons (SALW PoA) also led to politically binding commitments, the Small Arms Treaty was negotiated through the First Committee, albeit in parallel with the SALW PoA.[76] A Cyber PoA might thus at least inspire other initiatives, but the PoA itself will likely continue the focus on non-binding norms. Whether it will be established remains to be seen, though. The proposed PoA has been noted as a potential way forward in both the 2021 GGE[77] and the OEWG[78] reports, but the General Assembly has already adopted—against significant opposition—a resolution introduced by Russia convening a second OEWG from 2021-2025.[79] As of early 2022, the PoA has not been set up although its proponents remain committed to it.[80] Even if a Cyber PoA is adopted, it might simply replace the GGE, thus failing to achieve its primary goal of ending the dual-track process.

D. Addressing Cyber Election Interferences – Altering Values

The academic debate that has been triggered by digitalization and in particular by foreign election interferences has generated a significant number of contributions.[81] Some of these proposals,

[71]*See* OEWG Comments, *supra* note 51; OEWG Draft Substantive, *supra* note 52; OEWG Fifth Session, *supra* note 47.

[72]Joint Proposal, The Future of Discussions on ICTs and Cyberspace at the UN (Oct. 10, 2020) https://ceipfiles.s3.amazonaws.com/pdf/CyberNorms/UNGGE/Joint+Proposal_+The+Future+of+Discussions+on+ICTs+and+Cyberspace+at+the+UN.pdf.

[73]*Id.*

[74]*Id.*

[75]Aude Géry & François Delerue, *A New UN Path to Cyber Security,* DIRECTIONS BLOG (2020), https://directionsblog.eu/a-new-un-path-to-cyber-stability/.

[76]Informal Australian Research Paper, What Next for Advancing Responsible State Behaviour at the United Nations? 9 (Oct. 12, 2020) https://www.internationalcybertech.gov.au/sites/default/files/2020-12/australian-research-paper-what-next-advancing-responsible-state-behaviour-united-nations.pdf.

[77]GGE Report 2021, *supra* note 18, para. 97.

[78]OEWG Report, *supra* note 19, para. 77.

[79]G.A. Res 75/240, para. 1 (Dec. 31, 2020) (Yes: 92/No: 50/Abstentions: 21).

[80]Valentin Weber, *How to Strengthen the Program of Action of Advancing Responsible State Behavior in Cyberspace,* JUST SEC. (2022).

[81]*See, e.g.*, Russell Buchan, *Cyber Attacks: Unlawful Uses of Force or Prohibited Interventions?*, 17 J. CONFLICT & SEC. L. 212 (2012); Duncan Hollis, *The Influence of War; The War for Influence*, 32 TEMPLE INT'L & COMPAR. L.J. 31 (2018); Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARVARD NAT'L SEC. J. 146 (2018); Henning Lahmann, *Information Operations and the Question of Illegitimate Interference under International Law*, 53 ISRAEL L. REV. 189 (2020); Harriet Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention,* CHATHAM HOUSE (2019); JENS DAVID OHLIN, ELECTION INTERFERENCE - INTERNATIONAL LAW AND THE FUTURE OF DEMOCRACY (2020); Nicholas Tsagourias, *Electoral Cyber Interference, Self-Determination and the Principle of Non-intervention in Cyberspace*, *in* GOVERNING CYBERSPACE: BEHAVIOR, POWER AND DIPLOMACY (Dennis Broeders & Bibi van den Berg eds., 2020); Sean M Watts, *Low-intensity Cyber Operations and the Principle of Non-intervention*, *in* CYBER WAR: LAW AND ETHICS FOR VIRTUAL CONFLICTS (Jens David Ohlin, Kevin Goven & Claire Finkelstein eds., 2015).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

if implemented, would alter the values that are underlying the principle of non-intervention in its current form by introducing democratic values (I). Other proposals would indirectly advance a more robust understanding of sovereignty and non-intervention by aiming to reduce foreign participation in domestic discourses (II). The challenge posed by cyber election interferences thus finds diametrically opposed answers (III).

I. Introducing Democratic Values

International law is formally neutral among regime types. Each state is to be treated equally regardless of its political system[82] and every state may decide autonomously how to organize itself politically. This constitutes a central feature of an international legal system based on the sovereign equality of states.[83] By protecting each state's choice of a political system, the principle of non-intervention embodies the regime neutrality of international law. This regime neutrality has been challenged, in particular during the 1990s,[84] and it may have been abrogated from on a regional level.[85] But a universal entitlement to democratic governance suffers not only from a lack of an accepted definition of democracy,[86] it is also hardly reconcilable with a reality in which plenty of evidently non-democratic regimes represent states.[87]

The principle of non-intervention, of course, also protects a state's choice in favor of democratic governance. Protecting democratic discourse through the principle of non-intervention has, however, turned out to be a significant challenge. The principle of non-intervention protects the "exercise of [...] sovereign rights"[88] from undue interference. These sovereign rights are primarily exercised by the government as a representative of the state, or at least by state officials. The principle of non-intervention thus focuses on protecting state officials from direct interferences or, in cases of indirect intervention, from interferences that may not target state infrastructure but have repercussions on the agency of the state. This understanding makes it difficult to engage with election interferences that target voters in their decision-making process, as they are traditionally not understood to form part of the state. This is reflected in the differing statements by Western states that have been laid out above regarding which forms of election interference would be considered coercive.[89] Some states limit the scope to manipulations of election infrastructure, in other words, infrastructure that is administered by the state, while only a few states would also consider disinformation campaigns as possibly coercive. Those campaigns do not target state infrastructure, but the decision-making process of voters before they cast their ballot. And even in this case, Germany, for example, links the coercive effect of disinformation campaigns to the incitement of "violent political upheaval"[90] and thus the potential loss of authority of the executive. The fact that the principle of non-intervention is structurally blind to formations of the sovereign will outside of state structures may put democratic states at a disadvantage.

Nicolas Tsagourias has therefore suggested reappraising the principle of non-intervention in light of the principle of self-determination.[91] He argues that the right to self-determination

[82]G.A. Res. 2665(XXV), principle 6 (Oct. 24 1970) [hereinafter Friendly Relations Declaration].

[83]Nicar. v. U.S., 1986 I.C.J. para. 258.

[84]Thomas M. Franck, *The Emerging Right to Democratic Governance*, 86 Am. J. Int'l L. 46 (1992).

[85]*See, e.g.*, African Charter on Democracy and Good Governance, art. 2(1); Inter-American Democratic Charter, art. 1; Treaty on European Union, art. 2.

[86]Gregory H. Fox, *Democracy, Right to, International Protection,* Max Planck Encyclopedia of Public International Law, para. 6 (2008).

[87]Gregory H. Fox & Brad R. Roth, *The Dual Lives of "The Emerging Right to Democratic Governance",* 112 Am J. Int'l L. 67, 69 (2018).

[88]Friendly Relations Declaration, *supra* note 82, principle 3, para. 2.

[89]*See supra* at notes 31–36 and accompanying text.

[90]Germany, *supra* note 7, at 5.

[91]Tsagourias, *supra* note 81, at 51.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

does not cease after the creation of a state but continues to exist as a "right to authentic self-government, that is, the right of a people really and freely to choose its own political and economic regime",[92] which is protected by the principle of non-intervention.[93] According to this view, sovereign authority is primarily vested with the people, while the authority of the government is only derived. Consequently, "a government's authority and will remain free only when its sourcing is also free."[94] The primary object of protection is no longer the government, but "the people and the process of authority and will formation."[95] Thus, the process of derivation of authority—the election—falls within the scope of the principle of non-intervention.

Although this is not made explicit, Tsagourias' proposal would insert democratic values into the principle of non-intervention as it suggests that the authority of a government must be traced back to the people. This would substantially alter the underlying values of the norm which was supposed to preserve the free choice between different political systems. But to protect this choice, the outcome cannot be predetermined, which is why the source of a government's authority has so far not been considered. As a consequence, a cyber operation to overthrow a non-democratic government may become lawful.[96] This would be similar to Lori Fisler Damrosch's suggestion that nonforcible political influence is lawful when governments suppress the political rights of their peoples.[97] Damrosch wrote her article at the dawn of the cold war, contributing to a debate that culminated in the stipulation of the "emerging right to democratic governance."[98] Tsagourias, although seemingly taking up this debate, is not primarily concerned with spreading democratic values. His proposal is rather meant to protect those democracies that are already established. But even though it is primarily meant as a defensive concept, it is capable of being employed more offensively.

II. Shielding Domestic Discourses from Foreign Interference

The challenge of foreign election interferences has led other authors to propose at least indirect limitations to foreign participation in domestic political processes. Jens David Ohlin considers the Russian interferences in the 2016 US Presidential elections to have been a violation of the right to self-determination since outside actors "masquerading as inside members of the polity" participated in the political process.[99] He argues that not only the vote itself but also the preceding deliberative process should remain internal.[100] The participation of outside voices is not outright prohibited, but their origin, or at least the fact that they are not members of the polity, must be transparent.[101] Social media companies should therefore be required to label postings of a foreign origin.[102] But, distinguishing himself from the universalist claim made by Tsagourias, Ohlin explicitly argues that his understanding of self-determination only applies if a state is organized as an electoral democracy thus preserving a state's freedom to freely choose its political system.[103]

David Sloss similarly turns his attention from the content of harmful speech to the identity of the speaker.[104] But he takes the argument one step further suggesting to completely ban "Chinese

[92]Antonio Cassese, Self-Determination of Peoples: A Legal Reappraisal 137 (1995).
[93]Tsagourias, *supra* note 81, at 51.
[94]*Id.*
[95]*Id.* at 52.
[96]Tsagourias raises this question but ultimately leaves it unanswered, *see id.* at 57.
[97]Lori Fisler Damrosch, *Politics Across Borders: Non-Intervention and Non-Forcible Influence over Domestic Affairs*, 83 Am. J. Int'l L. 1, 37 (1989).
[98]*See* Franck, *supra* note 84.
[99]Ohlin, *supra* note 81, at 102.
[100]*Id.* at 127.
[101]*Id.* at 136.
[102]*Id.* Ohlin trusts that social media companies are technically capable of doing this.
[103]*Id.* at 97.
[104]David L. Sloss, Tyrants on Twitter: Protecting Democracies from Chinese and Russian Information Warfare 17 (2022).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

and Russian agents" from social media platforms.[105] To prevent these actors from relying on fictitious identities, he proposes that social media users must declare their nationality.[106] Member states of an "alliance of democratic states" will verify the declarations of their respective citizens.[107] In contrast to Ohlin, Sloss fears that social media companies are not capable of flagging foreign content on their own.[108] In addition, election-related content by social media users from "non-democratic states"—all states that are not members of the "Alliance"—will be flagged as being posted by a citizen of a non-democratic state.[109] Ohlin and Sloss sketch out a system in which certain speakers are excluded or limited solely based on their origin, not the content of their speech. While only Sloss goes as far as completely banning certain actors, both would require labeling foreign or "non-democratic" content. This constitutes an indirect limitation as it would stigmatize speech. It is meant to signal to the domestic audience that these forms of speech are less legitimate because they are foreign, in line with the premise that the deliberative process before an election should remain internal.[110]

The proposals by Ohlin and Sloss do not directly concern the principle of non-intervention. Sloss does not even rely on international law, but his ideas also rest on the premise that a political community may govern itself without participation from foreigners.[111] Ohlin rejects non-intervention as a useful framework for addressing election interferences.[112] The potential effect on the principle of non-intervention is rather an indirect one. The proposals, if implemented, would risk tipping the balance towards a much stronger understanding of sovereignty and the principle of non-intervention. The fact that "State sovereignty and international norms and principles that flow from sovereignty" apply to cyberspace constitutes by now established consensus.[113] As has been pointed out above, Western states have re-embraced the principle of non-intervention[114] and the protective dimension of sovereignty more generally.[115] Yet, this renewed focus on sovereignty is balanced with an emphasis on the free flow of information. Austria has explicitly highlighted that "State sovereignty must not serve as a pretext for tightening control over a State's citizens, which undermines their basic human rights such as the right to privacy and the freedom of expression,"[116] the latter consisting of the freedom to seek and receive information regardless of frontiers.[117] Similarly, the "EU has always advocated that the internet should be treated as one single unfragmented space, where all resources should be accessible in the same manner, irrespective of the location of the user or provider."[118] In contrast, other states have advanced a much more robust understanding of cyber sovereignty. For China, "Safeguarding Sovereignty and Security" is its primary strategic goal in cyberspace.[119] One manifestation of Chinese cyber sovereignty is the ability of states to "prohibit overseas organizations from fabricating and distorting facts and disseminating

[105] *Id.* at 159.
[106] *Id.* at 168.
[107] *Id.* At 169.
[108] *Id.* at 165.
[109] *Id.* at 156–157.
[110] See Franck, *supra* note 84.
[111] Sloss, *supra* note 104, at 11.
[112] Ohlin, *supra* note 81, at 88.
[113] GGE Report 2013, *supra* note 16, para. 19; G.A. Res 75/240 (Dec. 31, 2020).
[114] *See, e.g.,* New Zealand, *supra* note 22, para. 10; Germany *supra* note 7, at 5; *see also* France, *supra* note 22, at 7.
[115] Lahmann, *supra* note 46, at 90.
[116] Pre-Draft Report of the Open Ended Working Group Comments by Austria 3 (Mar. 31, 2020) https://front.un-arm.org/wp-content/uploads/2020/04/comments-by-austria.pdf.
[117] International Covenant on Civil and Political Rights, art. 19, Dec. 16, 1966, 999 U.N.T.S. 171.
[118] Patryk Pawlak, *Operational Guidance for the EU's International Cooperation on Cyber Capacity Building,* European Commission 39 (2018).
[119] International Strategy of Cooperation on Cyberspace, Chapter III.1 (2017) http://www.xinhuanet.com//english/china/2017-03/01/c_136094371.htm; *see also* Zhang Xinbao, *China's Strategy for International Cooperation on Cyberspace*, 16 Chinese J. Int'l L. 377, 380 (2017).

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

online information content in their territories that seriously damages their national security and public interests."[120] China's "great firewall" or "Golden Shield Project" allows it to control what information enters the country.[121] While the Chinese approach is limited to—extremely effective—content control, Russia and Iran have taken steps to completely disconnect their domestic networks from the global internet.[122] These understandings of cyber sovereignty do thus not give any regard to the free flow of information. Arguably, limiting this flow is one of its main purposes. This corresponds with other attempts at limiting foreign influence on domestic discourses. Various states such as China, Russia, Hungary, and Venezuela have passed legislation to restrict foreign funding for NGOs, which has also been interpreted as an expression of a more robust understanding of the principle of non-intervention.[123]

The proposals by Sloss and Ohlin are clearly less restrictive, but they still go in a similar direction by limiting the free flow of information. Focusing solely on the identity of the speaker, and not the content of speech, leads to blanket limitations that appear to be too restrictive. In trying to protect free and open discourses domestically, these limitations curtail the ability to lead free and open discourses transnationally and inadvertently advance a more robust understanding of sovereignty and the principle of non-intervention.

III. The Same Challenge – Diametrically Opposed Answers

Taking all the proposals discussed above together, a curious picture emerges. Since the end of the cold war, the promotion of democracy relied on de-emphasizing the principle of non-intervention. Democratic values were promoted by NGOs and other private actors to whom the principle did not apply.[124] The internet became part of that very promise.[125] The contemporary challenge for democratic states is a radically different one. Rather than exporting their ideals and values, they struggle to safeguard their own democratic structures that are under pressure, vulnerable precisely because of their openness. This leads to proposals that have direct or indirect repercussions on the values underlying the principle of non-intervention. Interestingly, even though the ideas discussed here all draw from the principle of self-determination, they lead to starkly different results. One, despite being conceived in a fairly defensive way, potentially justifies pro-democratic interventions reshaping the principle of non-intervention into a norm entrenched with democratic values. The principle of non-intervention would no longer be an obstacle to, but a vehicle for democracy promotion. The other proposals mark an inward turn. They would preserve the right of states to freely choose their political system, but in doing so risk giving up some of the foundational promises of the internet and lead from an interconnected world to a world of more closed, coexisting societies. The world thus envisioned is one that is paradoxically also advocated for by some of the authoritarian actors against which the proponents of the latter proposal wish to protect themselves.[126] It would be a world with sharp ideological differences in which a strong principle of non-intervention plays an important role in minimizing tensions—as it already has during the Cold War.[127]

[120]China's Views on the Application of the Principle of Sovereignty in Cyberspace 5 (2021) https://documents.unoda.org/wp-content/uploads/2021/12/Chinese-Position-Paper-on-the-Application-of-the-Principle-of-Sovereignty-ENG.pdf.

[121]Zhixiong Huang & Kubo Mačák, *Towards the International Rule of Law in Cyberspace: Contrasting Chinese and Western Approaches*, 16 CHINESE J. INT'L L. 271, 293 (2017).

[122]Justin Sherman, *Russia and Iran Plan to Fundamentally Isolate the Internet*, WIRED (Jun. 6, 2019) https://www.wired.com/story/russia-and-iran-plan-to-fundamentally-isolate-the-internet/.

[123]Krieger, *supra* note 12, at 991.

[124]*Id.* at 990.

[125]Lahmann, *supra* note 46, at 68.

[126]*See, e.g.*, Sergei Lavrov, *O праве, правах и правилах* (The Law, the Rights and the Rules) KOMMERSANT (Jun. 28, 2021) https://www.kommersant.ru/doc/4877702 ("The multipolar world is becoming reality").

[127]Krieger, *supra* note 12, at 990.

https://doi.org/10.1017/glj.2023.27 Published online by Cambridge University Press

E. Conclusion

Does digitalization reshape the principle of non-intervention? Does it create a new type of international law? Digitalization has sparked debates that have the potential to reshape the principle. Adopting a cyber treaty would change the nature of non-intervention in cyberspace, as would the expansion of informal rules. Incorporating democratic values would alter the central purpose of non-intervention as an embodiment of the regime neutrality of international law. Compared to that, advancing a more robust understanding of non-intervention seems much more conventional, even though the origin of certain proposals that at least have an indirect effect in that regard may be surprising. What has not changed, is the fact that geopolitical tensions surround the principle and the debate over its interpretation evidenced by the rivalries regarding the GGE/OEWG processes. The principle of non-intervention has always been politically charged and continues to be so. As a result, the principle's regulatory vagueness persists. But above all, digitalization has reinvigorated an old idea, namely that a certain sphere of a state's domestic affairs is protected from outside interference. The exact contours remain unclear, but the fact that there are limits somewhere is firmly accepted. Increasing interconnectedness does not make the principle of non-intervention obsolete, rather, it leads even Western states to rediscover the protective dimension of their sovereignty. While this rediscovery is currently limited to the cyber sphere, it coincides with more general perceptions that a rising "authoritarian international law" may lead to a reassertion of norms of noninterference,[128] or that "populist governments" re-advance a concept of international law as a law of coordination among independent nations.[129] Overly broad invocations of non-intervention in cyberspace[130] may therefore inadvertently reinforce trends towards a stronger non-intervention principle even outside the cyber context. Digitalization has, at least so far, not so much reshaped the principle of non-intervention, as it has given it a renewed emphasis. This has implications for the type of international law created by digitalization in general, where sovereignty and non-intervention may play a more prominent role again. The Westphalian castle is not so out of fashion after all.

Acknowledgement. The author would like to thank Janina Barkholdt and Sophie Schuberth as well as the convenors of this special issue for their valuable comments on earlier drafts of this paper.

Competing Interests. The authors declare none.

Funding Statement. No specific funding has been declared in relation to this article.

Note. This paper has been finalized in August 2021 with state practice cursorily being updated in June 2022.

[128]Ginsburg, *supra* note 1, 187.
[129]Krieger, *supra* note 12, 996.
[130]*See, e.g.*, France, *supra* note 22, at 7.

Cite this article: Willmer L (2023). Does Digitalization Reshape the Principle of Non-Intervention?. *German Law Journal* **24**, 508–521. https://doi.org/10.1017/glj.2023.27