The Cyber Dialogue at the Crossroads: Why States Disagree on the Need for a New Cyber Treaty?

Dmitry Krasikov[1,2], and *Nadezhda* Lipkina[1,*]

[1]Saratov State Law Academy, International Law Department, 410056 Saratov, Russia
[2]Institute of Scientific Information for Social Sciences of the Russian Academy of Sciences, 117218 Moscow, Russia

Abstract. As evidenced by the preliminary results of work of the UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security, currently the states have different views towards legal regulation of cyberspace. A number of states (mostly Western) argue that the existing international law sufficiently addresses the relationships in the area, and they call on all interesting parties to express their views on how the law is applied, while other states, like Russia, China and Venezuela claim that there is a legal vacuum as to the regulation of cyberspace and propose starting to globally negotiate a new binding legal instrument. This paper explores the reasons for the states to insist on their views on the need for a new cyber treaty and demonstrates that the respective disagreement between states cannot be explained neither by a global interest in maintaining the state of legal uncertainty about the proper sources or rules, nor by the lack of choice of the parties to the debate regarding the tools to address such uncertainty. The authors argue that the explanation lies in the correlation between corresponding substantive and instrumental stances of both sides of the debate, since the states' preferences regarding the appropriate rules can be more fully and effectively implemented within the respective instrumental solutions and such solutions provide their adherers with more tools to control the processes of their implementation.

1 Introduction

The problem of legal regulation of states' conduct in cyberspace has become a widely discussed issue. The very fact of the existence and growth of benefits and risks associated with development of information and communication technologies is undisputable and is the subject of international consensus (evidenced by the reports of the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (hereafter – GGE) and by the current work of the UN Open-ended Working Group on developments in the field of

*Corresponding author: n_lipkina@list.ru

information and telecommunications in the context of international security (hereafter – OEWG)). The role of legal instruments in preserving and developing these benefits and in mitigating the risks is also evident to all states. Nevertheless, states have different views towards legal regulation in this area: a number of states (including the United States, most European states, Australia and some others) argue that the existing international law sufficiently addresses the relationships in the area, while other states, like Russia, China and Venezuela claim that there is a legal vacuum as to the regulation of cyberspace [1, 2].

At the same time, certain states' belief in sufficiency of existing international law is accompanied by the recognition of the need to determine how exactly it regulates cyber conduct [3], while the other states' conviction as to the legal vacuum in the area do not prevent their insisting on applicability of certain existing rules (Russia and China highly endorse the principles of sovereignty and non-intervention in cyberspace [4]). Moreover, a number of those states who oppose the idea of a new treaty, do not consider this path as unacceptable per se, but declare that it is premature to discuss it (as do, for example, the United States and the United Kingdom).

The common point between the opposing views is the recognition of the lack of clarity (about the existence of applicable rules or how they are applied), and no one claims that nothing needs to be done about it. Therefore, the conflict of views on the issue of necessity and timeliness of a new treaty can be seen as a disagreement on the tools for eliminating the ambiguity of legal regulation of cyberspace (hereafter – the instrumental disagreement). At the same time, the states' views on material rules on cyberspace (either lex lata or lex ferenda) differ as well [4]. In particular, according to the states' comments on the pre-draft of the 2020 OEWG report, there are divergent views on applicability of the international humanitarian law, the right to self-defense and the rules on states' responsibility to cyberspace. Thus, the contradiction is twofold: the states do not only differ in their views on the applicable or proper sources of regulation but also on what the rules are or should be (hereafter – the substantive (or material) disagreement).

Maintaining the twofold contradiction obviously hinders the achievement of certainty which all states (as declared) are interested in, regardless of belonging to one side of the debate or another. Why to maintain the instrumental disagreement within this contradiction then? Why is it so important for states to insist on their instrumental views? If a state sees proper rules of conduct in cyberspace in one way or another, there seemingly should be no essential difference for it in what way its preferences will be endorsed – by a new treaty provision or by the way relevant for authoritative interpretation of the existing rules. An ideal way to solve the material contradiction would be to reach a consensus in that or another form (a treaty can be seen as a more preferable option from the standpoint of legal certainty [5]), but in any case, coordination of states' views is needed, and, arguably, the states have got tools to resist the unwanted rules in both approaches. Why, then, not to eliminate the instrumental disagreement for the sake of material dialogue?

The article contains the authors' opinion on the reasons for states to insist on their instrumental stances.

2 Methodology and Material Studied

The research is based on methods of analysis and synthesis, formal legal and comparative legal methods. The material studied includes the states' comments on the preliminary draft report of the 2020 UN Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (available at URL: https://www.un.org/disarmament/open-ended-working-group/), as well as the academic works on the issue of legal regulation of cyberspace.

3 Results and Discussion

The main idea of the article is that the disagreement between states as to the need to negotiate a new binding instrument on conduct in cyberspace is subordinate to their substantive debate on what rules should govern the area, and the states' respective standpoints on a new treaty serve as tools for upholding their interests regarding the material regulation.

3.1. The states' disagreements and the state of legal uncertainty

Modern.

It is a matter of broad consensus between states that the existence and development of information technologies and means of telecommunication carries not only advantages, but also risks.

In its Resolution 53/70 of 4 December 1998 'Developments in the field of information and telecommunications in the context of international security' the UN General Assembly expresses 'its concern that these technologies and means can potentially be used for purposes that are inconsistent with the objectives of maintaining international stability and security and may adversely affect the integrity of the infrastructure of States to the detriment of their security in both civil and military fields' and considers 'that it is necessary to prevent the use of information resources or technologies for criminal or terrorist purposes'. Basically, the same language can be found in a number of the UNGA resolutions on the issue adopted since 1998 (among the latest – Resolution 73/266 of 22 December 2018 and Resolution 73/266 of 2 January 2019). According to the UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, '[e]xisting and potential threats in the sphere of information security are among the most serious challenges of the twenty-first century'. The UN Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security is planning to include a special section on existing and potential threats in its report.

At the same time, states disagree on the legal means of eliminating and reducing the risks: some defend the need to adopt a new binding international instrument (a treaty), others consider the existing rules fully applicable to cyberspace and sufficient to address the risks, while recognizing the need for their clarification in terms of how they are applied to cyber conduct. This disagreement deepens the lack of clarity about how this behavior is regulated and whether it is regulated at all. Insisting on their views the states give birth to doubts about the ability of international law to properly address the risks. As Kubo Mačák puts it: "the reluctance of states to engage in international law-making has left a power vacuum, lending credence to claims that international law fails in addressing modern challenges posed by rapid technological development" [6]. Could it be that neither side makes concessions because both of them are interested in maintaining the state of uncertainty?

One potential advantage of the state of uncertainty is that it expands freedom of action: states can take certain actions that do not have a clear qualification, or can threaten to commit them, and the lack of clarity may calm their internal legitimacy concerns and, if necessary, allows them to insist on the legitimacy of their behavior in dialogue with other countries. In the absence of clear international legal framework, states feel free to adopt domestic legislation and to take measures subject only to constitutional constraints. Such circumstances are favorable for proliferation of mass surveillance, cyber espionage and sorts of practice that lie in the "grey zone" of international law. Samuli Haataja notes that "[i]n the context of states using cyber attacks against other states in their international

relations, the lower intensity forms of cyber attacks, while questionable, are often not specifically prohibited by international law and therefore regarded as permitted" [7]. According to M. Schmitt, "[t]he ongoing Snowden affair, which revealed widespread monitoring of activities abroad by the U.S. National Security Agency, illustrates the international community's unease with cyber operations that target other states or their citizens, even when nondestructive and, perhaps, lawful under current understandings of international law" [8]. The legality of cyber espionage under international law is also subject to the debate [9–11].

Besides, the absence of international control and clear mutual obligations prompts states to expand the extraterritorial effect of their legislation to protect themselves against external risks thereby expanding the boundaries of their jurisdictions. Stephen Townley argues that "states are increasingly acting as regulators at the international level (whether through international organizations or simply by virtue of the extraterritorial effects that their decisions may have)" [12].

In addition, the state of uncertainty and its maintenance can serve as a lever for pushing through one's preferences on material norms: it generates public criticism on states and can force them to make concessions on the substance of obligations in order to achieve certainty. According to E. Tikk and M. Kerttunen, 'the western rejection [of the cyber treaty negotiating initiative], as well as the argument of sufficiency of existing international law, can be seen as an attempt to avoid restraint. Accordingly, the West will have difficulties convincing the international community of its stand' [1].

Besides, a state of uncertainty on legal rules can be viewed as more advantageous in comparison with the emergence or approval of undesirable material norms: in the midst of disagreements between states regarding material regulation in cyberspace, one may prefer the lack of clarity to a clear and precise but unfavorable rule which the opponents insist on.

Nevertheless, these factors cannot be considered as advantages for each and every state: if all states were to a larger extent "cyber-like-minded" (regardless of belonging to one side of the debate or another), it is unlikely that the state of uncertainty could be their common choice. This is evidenced by the actual readiness to accept mutual legal obligations by states that have common views on the regulation of cyberspace.

First, the uncertainty obviously does not help in countering cyber threats, which are recognized with a certain degree of sincerity by all states. States have different views on values and corresponding cyber threats [2], but uncertainty does not eliminate the latters whatever they are. And although self-judgment and self-help is always available, the effect of measures taken by an injured state (such as countermeasures) in response to an allegedly wrongful conduct is diminished: the legitimacy of such measures is questionable as a result of doubts about the wrongfulness of the conduct, and as a consequence, their impact on the alleged violator is also limited.

Second, freedom of action can be an (equal) advantage only for states with equal opportunities, equally vulnerable and with similar interests, which is clearly not the case. Indeed, a cyber "savvy" state may be interested in a greater freedom of action, but at the same time such states are more sensitive to cyber risks (they are highly dependent on cyber infrastructure and are vulnerable to malicious treatment of their citizens, manufacturers and goods abroad), which forces them to seek compromises with each other and to remove uncertainty in mutual relations (e.g., the 2015 agreement between the United States and China concerning economic espionage), while remaining being opponents within the global debate.

Third, the benefits of uncertainty are not available to "conscientious" states or those sensitive to either internal or external pressure. If there are doubts about the legitimacy of a certain way of behavior, such states should be inclined to self-restraint. As a result, not only they do not take any advantage of uncertainty, but also may not allow themselves to behave

in a way that may raise external doubts as to its legitimacy. As for the assumption of uncertainty as a lever, it is potentially available only for states that are immune to public pressure: as a result of criticism about the unwillingness to negotiate clear rules, only states that are particularly susceptible to public opinion can consider themselves obliged to move forward, including through concessions.

W.H. Boothby notes that "[w]hether certain States do indeed see a narrow, national benefit in an absence of agreement as to the application of existing law is, and will remain, a matter of opinion" [13]. This paper shows that at least an assumption of a universal interest in maintaining a state of uncertainty about material norms applicable in cyberspace is erroneous and cannot serve as a plausible explanation for maintaining the instrumental disagreement between states.

3.2. The interrelation of instrumental and material disagreements: an absolute interdependence?

The disagreement between states regarding legal regulation of cyberspace is twofold: states have divergent views on the way of eliminating the state of uncertainty (or vacuum, as some see it) and on the substantive rules that determine international obligations in the field. Besides, the same groups of states oppose each other in both disagreements: those who advocate the need to negotiate an international treaty on cyberspace oppose the applicability of certain existing international rules to cyberspace, and vice versa.

There is an evident correlation between the respective positions within the instrumental and the material disagreements, but it should not be seen as an absolute interdependence. At first glance, it seems natural that insisting on inapplicability of certain existing norms, the respective states argue in favor of a new treaty: they believe that the corresponding relationships should be regulated differently than under the existing norms. For example, in its contribution to the discussion of the OEWG Draft Report China reiterated its position that "when it comes to state responsibility, which, unlike the law of armed conflicts or human rights, has not yet gained international consensus, there is no legal basis at all for any discussion on its application in cyberspace" and also proposed developing a universally-accepted approach to attribution of conduct under the auspices of the UN.

However, it cannot be assumed that advancing a position on any rules which are different than the existing ones necessarily involves insisting on a new treaty. In other words, it would be incorrect to believe that the option proposed by the opponents of a new binding instrument totally excludes the possibility to recognize that the existing substantive rules operate differently than in other areas, or to conclude that any of such rule is in whole or in part inapplicable to cyberspace. To take the interpretation path and to stop insisting on a new treaty would not automatically mean recognizing the applicability of all existing rules in the same way that they apply to noncyber relationships. The interpretation path supporters call on states to express their views on the matter, and the views can be different, which affects the way these rules are applied. The positions of states are of fundamental importance for formation of customary law and can influence the interpretation of existing norms according to the 1969 Vienna Convention of the Law of Treaties. The concept of evolutionary interpretation [14] proceed from the legal rules' potential to evolve, and this process involves a significant convergence of the states' practice and attitudes. Thus, there is no absolute interdependence between the views of the supporters of a new treaty and their preferences about the proper rules of conduct in cyberspace, since the interpretation path does not totally deprive them of the possibility to defend their views on material regulation.

Even more evident is the absence of absolute interdependence between the instrumental and material positions of the opponents of a new treaty. Drafting a new treaty assumes the

participation of all interested parties and allows states to express any views about any preferred rules. Accordingly, such states' advancing their vision of proper substantive legal norms can well be realized within the process of developing a new treaty. For example, nothing prevents them from promoting the right to self-defense in cyberspace while negotiating a treaty.

The above considerations do not assess the advantages of the sides of the debate to make concessions related to the regulatory instruments but are intended to demonstrate the absence of an absolute interdependence between the correlated views within the two disagreements between states. The main conclusion is that the preservation of the instrumental disagreement cannot be explained not only by a kind of global interest in maintaining the state of uncertainty, but also by the lack of choice of the participants in the discussion regarding the tools to address the uncertainty. The explanation is that the respective instrumental stances provide the parties to the debate with corresponding comparative advantages as to promotion their material preferences, which is subject to discussion in the next section.

3.3. The interrelation of instrumental and material disagreements: the states' comparative advantages

States express opposing views regarding certain appropriate substantive rules of conduct in cyberspace and insist on different ways to overcome the disagreement. At the same time, it cannot be considered that defending one or another material position is totally incompatible with implementation of any of the two opposing instrumental options. Despite the negative consequences of the state of uncertainty generated by the instrumental controversion, it still exists, and the states continue to maintain it. This paper argues that the explanation lies in the correlation between corresponding material and instrumental stances of both sides of the debate: first, their preferences regarding the appropriate rules can be more fully and effectively implemented within the respective instrumental solutions, and, second, such solutions provide their adherers with more tools to control the processes of their implementation.

Potentially, the material preferences of the opponents of a new treaty can be satisfied in such treaty. The parties to the drafting process, using with their status and advantages, can put efforts in defending their preferences on the range of rules and scope of their operation, their content and relationship with existing international law; they can block negotiations, bargain for advantageous solutions in the field and even elsewhere. That would be easier if the states did not have any material disagreements, but at the same time, the latter does not allow their material views to automatically prevail in either instrumental option. Nevertheless, even if we assume that such states can successfully use their negotiating capabilities as to the material norms in the process of a treaty drafting, the interpretation path is still more advantageous for them: if we compare the effects of (potential) implementation of the two instrumental scenarios, it becomes clear that the realistic spectrum and scope of rules, as well as the effects of their approval would be different.

Firstly, it seems unrealistic to cover all the material preferences of the new treaty opponents with a single legal instrument. In particular, it is difficult to imagine how to incorporate into a separate treaty the entire volume of international humanitarian law, as well as the law on the responsibility of states and all other rules that this group of states perceive as applicable to cyberspace. Of course, the treaty may contain special rules governing its interaction with other sources of international obligations in an abstract manner (as does, for instance, the 1982 UN Convention on the Law of the Sea), but this would still leave open the issue of applicability of such other sources to cyberspace (if and

to the extent this issue is open at present), basically returning the debate to the present stage.

Secondly, to recognize the applicability of the existing norms to cyberspace (even in certain specific or modified form) is to presume that all the participating states have corresponding rights and obligations (derived from the UN Charter, humanitarian convention, etc.), while a new treaty not only needs to be adopted but also should be ratified to create any obligations, and, viewed realistically, a number of potential parties will be narrower compared to the existing rules. Besides, it is alleged that "[e]ven if states were to embark on multilateral diplomatic conferences with the aim of concluding cyber treaties, any resulting treaty would likely be perforated with individual reservations, thereby degrading its practical effect" [15].

Thirdly, the recognition of the applicability of the existing rules to cyberspace as a result of their interpretation and with the help of soft law instruments brings into this area not only the rules themselves, but also their entire context, history of adoption, practice of application and interpretation with all the certainty achieved (albeit with all grey zones). On the contrary, consolidation within a new agreement of any rules that seem identical to their "predecessors" will surround them with new context, goals and object, drafting history, etc., and, as a result, the rules which are prima facie the same, may appear to be effectively different.

Fourthly, taking into account the rational doubts on the possibility to globally reconcile the material positions on new binding rules [2, 16], any concession of the current opponents to a new treaty to start negotiations could be seen as even deepening the state of legal uncertainty in the area.

These factors, among others, force the opponents of the new treaty to insist on their instrumental path, despite the negative effects of the ongoing debate and the state of uncertainty it generates.

A similar rationale determines the benefits of negotiating a new treaty for the proponents of such initiative: the potential choice of this path and its implementation will have a significant restrictive effect on the applicability of existing regulations. Even reaching an agreement on the need to develop a new treaty in itself can reinforce doubts on the applicability of the existing norms of international law on controversial issues (especially those that the participants will put up for discussion). At the same time, even inclusion of provisions in the proposed agreement that are essentially similar to the current rules is incapable of fully translating their content and their subjects into the area, as noted above. In addition, for the supporters of a new treaty, insisting on this option becomes an important strategy for defending their material positions, since the very idea of a treaty raises doubts if the existing rules are applicable.

Inequality of the disputing states' capabilities of control over formation and approval of rules within the two scenarios is another important explanation for the persistence of the instrumental contradiction. Such capabilities are stronger for states that refuse to recognize the necessity and timeliness of a new treaty and insisting on this view is an effective tool for its supporters to promote their material preferences.

The new treaty opponents have got an obvious advantage regarding the choice of the instrumental path itself, and it makes little sense to abandon it, since they largely control this choice itself. Seen as preferred by a substantial part of the international community, the option of existing rules' interpretation supplemented by soft law tools is a way to move forward that can and will be implemented by default, since there is no effective way for any opposing state or group of states to prevent its implementation and to fully ignore this process. The supporters of a new treaty need a positive consent of a significant number of states on and for its effective implementation, while the opponents do not need anything to do for their view to prevail except objecting to the new treaty initiative. The effect is that

any state's attitude towards legal regulation of cyberspace and any kind of its behavior in the area, in fact, automatically follows the interpretation path. In addition, unlike objections to a new binding legal instrument, there can be no justified objections to interpretation as such, and any related accusations of maintaining the state of uncertainty are leveled by the fact that such new instrument opponents do not speak out against it in principle, but argue that this is a premature initiative and it is first necessary to understand how the existing law is applied to cyberspace. Additionally, any doubts in moral legitimacy of the objections to a new treaty are reduced by the respective states' insisting on the applicability of existing norms and by the political achievements (including the adoption of "voluntary, non-binding norms of responsible State behavior").

Also, the opponents to a new treaty have greater control over the implementation of their option to eliminate the legal uncertainty. Interpretation, supplemented by the development of non-binding rules, allows the existing rules to evolve or new rules to appear gradually, which is not the case within the path of a new instrument drafting, since the latter is a more or less comprehensive package deal.

Besides, since the participation of opponents of a treaty in the development of non-binding political commitments is linked to their insistence on applicability of existing norms, from the moral point of view their position does not look unattractive. They are convinced that there is no vacuum or gap in regulation, and therefore, if they should feel responsible for the consequences of the instrumental disagreement, it is only for the state of uncertainty regarding the legal vacuum, and not for the legal vacuum as such (if it exists, as the other side of the debate claims).

Under these circumstances, and taking into account the material preferences of the supporters of the treaty path, their instrumental position, is, among other things, an attempt to resist the imbalance of control over the formation and approval of rules: for such states which are basically forced to obey the scenario of their opponents, insisting on a new treaty is the most effective tool of defending their material positions and an attempt to gain some political points.

4 Conclusions

This paper demonstrates that the instrumental disagreement between states as to regulation of their conduct in cyberspace cannot be explained neither by a global interest in maintaining the state of legal uncertainty about the proper sources or rules, nor by the lack of choice of the participants in the discussion regarding the tools to address such uncertainty. The explanation lies in the correlation between corresponding material and instrumental stances of both sides of the debate, since the states' preferences regarding the appropriate rules can be more fully and effectively implemented within the respective instrumental solutions and such solutions provide their adherers with more tools to control the processes of their implementation.

Acknowledgements

The present paper is a part of the project "Theory-to-practice model of endorsement of territorial sovereignty and delimitation of States' jurisdictions in cyberspace" supported by the Russian Foundation for Basic Research (RFBR Grant No. 20-011-00806).

References

1. E. Tikk, M. Kerttunen,(2018), https://cpi.ee/

2. I.Stadnik, Masaryk Univ. J. of Law and Tech., **11(1)**(2017)
3. H. Moynihan, *The Application of International Law to State Cyberattacks: Sovereignty and Non-intervention* (2019)
4. D. Broeders, L. Adamson, R. Creemers,(2019)https://www.thehaguecybernorms.nl/
5. M.Eilstrup-Sangiovanni, Philosophy & Tech., **31**(2018)
6. K. Mačák, Leiden J. of Int. Law, **30(4)**(2017)
7. S. Haataja,*Cyber Attacks and International Law on the Use of Force*(2019)
8. M.N. Schmitt, Stanford Law & Policy Rev., **25(2)** (2014)
9. W.C. Banks, Emory Law J., **66(3)**(2017)
10. N. Jupillat,North Carolina J. of Int. Law and Comm.Regulation, **42(4)**(2017)
11. A. Lubin, Int.Law Students Association Quarterly, **24(3)**(2016)
12. S.Townley, Chicago J. of Int. Law, **18(2)**(2018)
13. W.H. Boothby,*New Technologies and the Law in War and Peace* (2019)
14. G.Abi-Saab, K.Keith, G.Marceau, C.Marquet, *Evolutionary Interpretation and International Law*(2019)
15. A.-M. Osula, H. Rõigas, *International Cyber Norms: Legal, Policy & Industry Perspectives*(2016)
16. D. Jinks(2018)https://www.justsecurity.org/