THE TALLINN PAPERS

A NATO CCD COE Publication on Strategic Cyber Security

WOLFF HEINTSCHEL VON HEINEGG

INTERNATIONAL LAW AND INTERNATIONAL INFORMATION SECURITY: A RESPONSE TO KRUTSKIKH AND STRELTSOV

Tallinn Paper No. 9
2015

CCDCOE
NATO Cooperative Cyber Defence Centre of Excellence Tallinn, Estonia

Previously in This Series

No. 1 Kenneth Geers "Pandemonium: Nation States, National Security, and the Internet" (2014)

No. 2 Liis Vihul "The Liability of Software Manufacturers for Defective Products" (2014)

No. 3 Hannes Krause "NATO on Its Way Towards a Comfort Zone in Cyber Defence" (2014)

No. 4 Liina Areng "Lilliputian States in Digital Affairs and Cyber Security" (2014)

No. 5 Michael N. Schmitt and Liis Vihul "The Nature of International Law Cyber Norms" (2014)

No. 6 Jeffrey Carr "Responsible Attribution: A Prerequisite for Accountability" (2014)

No. 7 Michael N. Schmitt "The Law of Cyber Targeting" (2015)

No. 8 James A. Lewis "The Role of Offensive Cyber Operations in NATO's Collective Defence" (2015)

The Tallinn Papers

The NATO CCD COE's *Tallinn Papers* are designed to inform strategic dialogue regarding cyber security within the Alliance and beyond. They address cyber security from a multidisciplinary perspective by examining a wide range of issues, including cyber threat assessment, domestic and international legal dilemmas, governance matters, assignment of roles and responsibilities for the cyber domain, the militarisation of cyberspace, and technical. Focussing on the most pressing cyber security debates, the Tallinn Papers aim to support the creation of a legal and policy architecture that is responsive to the peculiar challenges of cyberspace. With their future-looking approach, they seek to raise awareness and to provoke the critical thinking that is required for well-informed decision-making on the political and strategic levels.

Submissions

The Tallinn Papers is a peer reviewed publication of the NATO Cooperative Cyber Defence Centre of Excellence. Although submissions are primarily commissioned by-invitation, proposals consistent with the annual theme and dealing with issues of strategic importance will be considered on an exceptional basis. Since the Tallinn Papers are meant for a wide audience, such proposals should assume no prior specialised knowledge on the part of the readership. Authors wishing to submit a proposal may contact the Editor-in-Chief at publications@ccdcoe.org.

International Law and International Information Security: A Response to Krutskikh and Streltsov

Wolff Heintschel von Heinegg[1]

In their 2014 article,[2] Andrey Krutskikh and Anatoly Streltsov address the relationship between international information security and international law. The purpose of the article seems to be either to advocate a new international legal framework for the use of information and communication technologies (ICTs), or to support considerable amendment of the existing principles and rules, in particular those of the *jus ad bellum* and the *jus in bello*. Although the authors stress the necessity of preserving the peremptory norms of the UN Charter, such as as non-intervention and prohibition of the use or threat of force, they begin from the premise that there is a "lack of a full-fledged international legal framework governing ICT-related activities by States, including their military aspects."[3]

In support of their plea for a new or modified international legal framework, Krutskikh and Streltsov pose 27 questions. Unfortunately, they fail to provide answers to all of them and sometimes obfuscate, rather than clarify, the legal issues at hand. Interestingly, the *Tallinn Manual*,[4] a logical and suitable basis for discussion with regard to the applicability of the *jus ad bellum* and the *jus in bello* to cyber operations, is mentioned, but is not taken into meaningful consideration.

1 Senior Fellow, NATO Cooperative Cyber Defence Centre of Excellence; Professor of Public Law, in particular Public International Law, European Law and Foreign Constitutional Law, Europa-Universität Viadrina, Germany.

2 Andrey Krutskikh and Anatoly Streltsov, 'International Law and the Problem of International Information Security', 60 *International Affairs* 64-76 (No. 6, 2014). The article is available at https://ccdcoe.org/sites/default/files/multimedia/pdf/International_Affairs_No6_2014_International_Law.pdf. *International Affairs* is the English edition of the Russian journal *Mezdunarodnaia zhizn*, which is published by the Ministry of Foreign Affairs of the Russian Federation. The Russian Minister of Foreign Affairs is *ex officio* head of the journal's board of editors.

3 *Ibid*., pp. 64, 75.

4 *Tallinn Manual on the International Law Applicable to Cyber Warfare* [hereinafter *Tallinn Manual*], Michael N. Schmitt (gen. ed.), Cambridge University Press, 2013. The author served as a member of the International Group of Experts who drafted the *Tallinn Manual*.

The authors take the position that the *Tallinn Manual* is an effort by "NATO experts" who are "diametrically opposed [to Russia's] policy of averting military and political confrontations in information space" because Russia "believes that the top priority is to anchor the rules of prevention of conflicts arising from the unlawful use of ICTs in international law."[5] Apart from the fact that the *Tallinn Manual* was not drafted by "NATO experts", but rather by independent international experts, it is difficult to comprehend why the authors ignore it altogether, in particular when they discuss, *inter alia*, whether and to what extent cyber operations might qualify as "armed attacks" triggering a state's right of self-defence. One cannot escape the impression that the authors consider the comprehensive and nuanced answers provided by the *Tallinn Manual*, in particular the commentary on the black letter rules, as running counter to their objective of modelling international law in a manner that serves the interests of the Russian Federation, as distinct from those of what the authors refer to as "the West". Perhaps they dismiss the existing international legal framework as inadequate because they eventually hope for a total ban on the military uses of cyberspace.

That said, the questions the authors pose and the answers thereto are neither irrelevant, nor to be rejected entirely. They discuss important aspects of the *jus ad bellum,* the *jus in bello* and other basic rules of international law, such as sovereignty. They purportedly base their arguments on the *lex lata*. In doing so, they adopt a particular understanding of the existing principles and rules of international law that should not go unanswered. This Tallinn Paper analyses some of the questions and answers with an eye towards identifying points of convergence and divergence.

This response does not address questions 20 or 24 to 26, either because they do not relate to genuinely international legal issues, or because the authors have failed to proffer any answer. Question 27 pertains to a possible update of the definition of ICTs with a view to including robotic engineering and artificial intelligence. It appears as if the authors hope to pave the way for yet another international ban of a technology, the development of which is mainly in the hands of states other than the Russian Federation. Question 21 relates to efforts that should be undertaken to prevent the use of ICTs for terrorist and criminal purposes. Their answer is essentially limited to rejection of the Council of Europe's Convention on Cybercrime (Budapest Convention, 2001), thereby echoing Russian reservations. The authors take the view that the Budapest

5 *Supra* note 2, p. 75.

Convention is irreconcilable with the principle of sovereignty, that it could be an attempt to legalise "global espionage", and that it lacks provisions on anti-spam measures. They prefer a universal convention on cybercrime that would address these concerns. This represents yet another attempt to extend state control over cyberspace, in a manner that goes far beyond what is necessary for international information security and jeopardises the economic and social benefits of a free cyberspace.

Unlawful Uses of ICTs

The authors use the phrase "unlawful uses of ICTs" throughout the article. Their characterisation of ICTs as "unlawful" is premature if the use of cyber means is still to be evaluated in the light of international law. In any event, it is unclear what the authors mean by "unlawful uses" or to which cyber operations they are referring. Presumably, the phrase is used to encompass a wide array of cyber operations attributable to states and presumes their incompatibility with international law.

Adequacy of the Present System of International Law

Question 1 appears to deal with the adequacy of the present international legal system for regulating "unlawful uses of ICTs"; the accompanying answer is far from comprehensive. Of course, it is difficult to establish whether a cyber operation qualifies as a use of force or an armed attack pursuant to Articles 2(4) and 51 of the UN Charter, respectively. In this regard, and despite what the authors seem to suggest, a "breach of the territorial borders" of the victim state is not required to qualify it as such. Perhaps what they mean to imply is that a cyber attack need not necessarily result in material damage or materialise outside cyberspace to cross these thresholds, or that "force" can be implicated remotely without having to physically enter another state's territory.

The definitional issue aside, there is general agreement that the existing principles and rules of international law apply to cyberspace and to state conduct in or through cyberspace. As the International Court of Justice rightly emphasised in its Advisory Opinion on Nuclear Weapons, "the established principles and rules of humanitarian law […] apply to all forms of warfare, and to all kinds of weapons, those of the past, those of the present and those of the future."[6]

6 Legality of the Threat or Use of Nuclear Weapons, Advisory Opinion, 1996 I.C.J. 226, para. 86 (July 8).

State practice seems to confirm that the existing *jus ad bellum* and other norms of international law are, in principle, adequate and sufficient to regulate state cyber conduct.[7] Nevertheless, states must continue to cooperate in forging consensus over how these principles and rules apply to cyberspace. The position of the authors on this matter is far from clear. On one hand, they are willing to apply the "*jus cogens*, arising from the UN Charter"[8] to cyberspace. On the other, they advocate, at minimum, modification of existing rules and, maximally, a new universal international legal framework that would include unspecified arms control aspects.

In this context, question 10 merits comment. While not clearly formulated, it bears on the characterisation of a cyber operation as terrorist or criminal in character. The authors believe that such a characterisation enables the target state to respond without being restricted by international law, even though the response might pose a threat to international peace and security. This is a tenuous position. If the response to a criminal or terrorist cyber operation poses a threat to international peace and security, it must be evaluated in light of the *jus ad bellum*. Moreover, international law governs any response to a criminal or terrorist cyber operation that involves the rights and interests of other states. This is so despite the fact that the response is primarily targeted against a non-state actor. The aforementioned UN Charter provisions are central in this regard.

Jus ad Bellum: Cyber Operations Qualifying as Use of Force, Act of Aggression or Armed Attack

Six questions – 2, 3, 4, 5, 6 and 11 – explicitly deal with the *jus ad bellum*, that is, the issues when a cyber operation qualifies as a use of force, an act of aggression, or armed attack.

It is untenable to suggest, as the authors have in their answer to question 1, that a "war waged […] to defeat the adversary violates the UN Charter and the principle of sovereign equality of states."[9] War is never commenced – whether legally or illegally – with a view to losing. The statement sheds light on the authors' principal approach to the applicability of the *jus ad bellum* to cyberspace, one that seems designed to prevent technological inferiority rather than contribute to the

7 See various national cyber security strategies that are available at: https://ccdcoe.org/strategies-policies.html.

8 *Supra* note 2, p. 75 [italicisation added].

9 *Supra* note 2, p. 66.

enhancement of international (cyber) security.

A similar approach has seemingly been taken in the answer to question 3 on whether the term "weapon" applies to ICTs. In consonance with an agreement of the Commonwealth of Independent States (CIS),[10] the authors define the term "information weapon" as "information technologies, means and methods applied for the purpose of information war."[11] With regard to the term "information war", they rely on a different agreement[12] according to which:

> "…the characteristics of information war include the impact on transportation, communication and air control systems, missile defense and other types of defense facilities as a result of which the State loses its defense capabilities in the face of an aggressor and fails to exercise its legitimate right to self-defense, breaching information infrastructure operation, which leads to the collapse of administrative and decision-making systems in the states, and computer attacks on critically important structures."[13]

Although there is an undeniable tendency amongst states to include such cyber operations in the notions of "use of force" or even "armed attack", it is far from settled whether the definitions can be considered as properly reflecting contemporary international law. Moreover, the definition of "information war" is inadequately linked to a loss of defence capabilities. This discussion demonstrates that the term "information war" is too vague to contribute to a clarification of the scope of applicability of the *jus ad bellum* to cyberspace; accordingly it should be avoided.

Question 11 addresses the critical issue whether a cyber operation qualifies as a use of force in accordance with Article 2(4) of the UN Charter. The authors unfortunately provide no answer. Instead, their focus is on the notions of "act of aggression" and "armed attack".

The notion "act of aggression" is dealt with in questions 2 and 4. In their answer to question 2, the authors take the position that Article 2 of the Definition of

10 The authors rely on the annex to the Agreement on Cooperation of the CIS members in the field of information security, St. Petersburg, 20 November 2013.

11 *Supra* note 2, p. 67.

12 Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of Ensuring International Information Security, Yekaterinburg, 16 June 2009.

13 *Supra* note 2, p. 67. Also, Annex 2 to the Agreement between the Governments of the Member States of the Shanghai Cooperation Organization on Cooperation in the Field of International Information Security.

Aggression[14] can be applied to cyber operations, but must be "adapted to the specific attributes of ICTs"[15], in particular those lacking kinetic effects. While this may well be, it should not be forgotten that the primary purpose of the Definition of Aggression is to provide guidance to the UN Security Council in determining the existence of one of the conditions laid down in Article 39 of the UN Charter for taking action to maintain or restore international peace and security. Of course, the Definition has regularly been taken into consideration in order to establish whether an armed attack has occurred,[16] but having the UN General Assembly provide a new definition of aggression that includes certain cyber operations would be a dangerous precedent. States make international law; they should not surrender this prerogative to a body that is political in nature, the decisions of which will only in most exceptional cases be acceptable to the entire community of states. Moreover, it is doubtful whether there is a need for amendment or modification of the General Assembly resolution. As demonstrated by the *Tallinn Manual*, the foundational terms of the *jus ad bellum* – "use of force" and "armed attack" – can be interpreted in the cyber context on their own merits and in the light of subsequent state practice.[17]

While question 4 also deals with the term "act of aggression", its focus lies on self-defence and on the term "armed attack". The right of self-defence is also addressed in questions 5 and 6. The authors rightly emphasise that in view of the fact that cyber operations often have no kinetic effects, it is difficult to establish whether they qualify as "armed attacks". Hence, there is a need to identify criteria for determining whether a cyber operation can be assimilated to a kinetic armed attack. The fact that the authors, by way of example, refer to "leaks of classified information on Wikileaks website"[18] in this context is worrying. The disclosure of classified information by foreign state organs may qualify as a violation of sovereignty, but hardly as a use of force or, *a fortiori*, an armed attack.

In their answer to question 4, the authors also criticise NATO for having extended Article 5 of the North Atlantic Treaty to cyberspace. They assert that the decision "runs counter to the NATO members' stance which rests on the

14 Annex to UN GA Resolution 3314 (XXIX) of 12 December 1974.

15 *Supra* note 2, p. 66.

16 See, *inter alia*, *Military and Paramilitary Activities in and against Nicaragua (Nicar. v. U.S)*, 1986 I.C.J. 14, para. 191 (June 27); *Armed Activities on the Territory of the Congo (Dem. Rep. Congo v. Uganda)*, 2005 I.C.J. 168, paras. 146-47 (Dec. 19).

17 *Tallinn Manual*, *supra* note 3, p. 42 *et seq.*

18 *Supra* note 2, p. 67.

assumption that there is no need to elaborate new treaties in the use of ICTs and that existing norms of international law can be applied "automatically.""[19] This leads to the conclusion that the authors deny other states the right to exercise their sovereign right of authentically interpreting Article 51 of the UN Charter, although they appear willing to grant that right to the Commonwealth of Independent States and the Russian Federation. Apart from this incongruence, their criticism is unfounded. Article 5 of the Washington Treaty is based on Article 51 of the UN Charter and the corresponding customary international law. It is difficult to see why applicability of the right of collective self-defence to cyberspace, which is rather limited in nature and scope, is not reconcilable with the view that existing norms of international law are suitable for regulating state conduct in and through cyberspace.

The authors seem to be unwilling to accept application of the right of self-defence to cyber operations unless agreed upon in either a treaty or an international forum, such as the UN General Assembly. Therefore, in their answer to question 5 (which, among others, relates to the right of self-defence), the authors take the position that Iran cannot "file a complaint to the International Court of Justice against […] countries charging them with the Stuxnet attack" because there is a "lack of international legal regulation in this field as well as relevant precedents."[20] It may be that the authors are unprepared to consider the Stuxnet operation an armed attack in the sense of Article 51 of the UN Charter. Whether this is the case or not, the exercise of the right to self-defence is not dependent on any proceedings before the International Court of Justice. This raises the question of why referral is made at all. All in all, the authors provide no answer to that question. They would have been better served by consulting the *Tallinn Manual* and setting forth their agreement or disagreement with its Rules and commentary on point, and doing so would have contributed to the necessary legal discourse. Passing comments and insinuations is far from helpful.

Finally, question 6's answer regarding the prevention of states' misuse of the right of self-defence in or with regard to cyberspace adds little to the discussion. The authors again emphasise the necessity of elaborating "the criteria for the rationale and proportionality of the reaction."[21] Insofar as this means that states should agree on criteria for establishing whether a cyber operation constitutes an armed attack, the authors cannot be criticised. Such an effort would certainly

19 *Ibid*., p. 68.

20 *Ibid.*

21 *Ibid.*

add to legal clarity. It may be added, however, that it is more than uncertain whether states are prepared to agree on an interpretation of cyber armed attack going beyond what they have agreed upon in Article 51 of the UN Charter. It would set a bad precedent. Because the authors reject any interpretation that is not agreed upon either in a treaty or an international forum, each time a new technology comes into existence there would have to be a formal consensual interpretation. It is also impossible to provide specific and objective criteria for the determination of the proportionality of an act of self-defence. Proportionality is, and will continue to be, based on circumstance. Any endeavour to contain it by objective and absolute criteria would render the right of self-defence an empty shell.

Jus in Bello

Five questions – 7, 8, 9, 16 and 17 – address the *jus in bello*, also labelled international humanitarian law or the law of armed conflict. The law of neutrality seems to be dealt with in question 15.

Question 17 relates to identification of the "theatre of war" in cyberspace. Again, the authors are satisfied to pose the question without providing an answer. The question may hint at the problematic issue of determining the geographic boundaries of an armed conflict and the related matter of the geographic scope of application of the law of armed conflict. Unsurprisingly, the authors appear unwilling to take a position, but then they favour the demilitarisation of cyberspace. A clarification of the scope of applicability of the law of armed conflict to cyberspace might run counter to efforts aimed at eliminating its military use. However, such a demilitarisation – in whatever form it might take – is simply unattainable in the near or mid-term future. Almost all armed forces of the world make use of ICT and conduct, or plan to conduct, operations in or through cyberspace. Therefore, there is no doubt that cyberspace is part of the modern "battlefield" and that, accordingly, the law of armed conflict applies to military cyber operations during an armed conflict. A different question is whether cyber operations alone can bring an armed conflict into existence.[22] This is addressed only indirectly in question 7, but, again, is left unanswered by the authors.

Questions 7 and 8 address the issue of whether, and if so what, enemy cyber infrastructure qualifies as a lawful military objective which may be attacked

22 See *Tallinn Manual*, *supra* note 3, p. 79 *et seq.* and p. 84 *et seq.*

by traditional (kinetic) means of warfare (question 7), or is a protected object pursuant to law of armed conflict (question 8). The authors take no position on the former, although the answer is obvious. Article 52(2) of the 1977 Additional Protocol I, which the Russian Federation ratified on 29 September 1989, sets out the definition of lawful military objectives. Again, the lack of an answer seems motivated by the goal of demilitarisation of cyberspace.

In their answer to question 8, the authors take the view that "the norms of international humanitarian law have to be considerably adapted to the progress in the use of ICTs."[23] Although the question relates to cyber infrastructure – that is, to the physical layer of cyberspace – the claim for an amendment of the existing law of armed conflict is justified by reference to the logical layer of cyberspace. It is true that at present data is not (yet) considered to be an objects.[24] However, with regard to physical cyber infrastructure, if it does not qualify as a military objective, then it is a civilian object protected against attack. The authors' answer is therefore evasive, a further indication of the extent to which they are unwilling to admit the applicability of the law of armed conflict to cyberspace.

It is, therefore, entirely consistent that the authors fail to answer questions 9 and 16, which deal with the principles of distinction and proportionality. Yet, it must be emphasised that these fundamental principles of the law of armed conflict apply to military operations in and through cyberspace.[25] While the characteristics of cyberspace may make it difficult to identify lawful targets and to avoid or minimise excessive collateral damage, such difficulties do not absolve the parties to a conflict from their obligations.

It is unclear whether question 15 addresses the position of a neutral state during an international armed conflict. At first glance, it concerns the difficulties of preserving the neutral status of third states when parties to a conflict use the cyber infrastructure located in that third state. In light of the last part of the question, which links such use to a violation of international peace and security, it seems to extend far beyond the law of neutrality. The use of neutral cyber infrastructure for the exercise of belligerent rights, including attacks, is undeniably a legal problem. In that regard, the authors are correct. It is, however, unhelpful that they merely highlight the difficulties without providing even rudimentary answers. Again, reference to the *Tallinn Manual*'s treatment of the

23 *Supra* note 2, p. 69.

24 See *Tallinn Manual*, *supra* note 3, p. 127.

25 *Tallinn Manual*, *supra* note 3, p. 110 *et seq.* and p. 159 *et seq.*

subject would have been appropriate.[26] It needs to be emphasised that a state is not in violation of its obligations under the law of neutrality if it does not constantly monitor the data traffic routed through its cyber infrastructure; a neutral state is merely obliged to terminate an exercise of belligerent activity of which it has positive or constructive knowledge.

Attribution and State Responsibility

Questions 12, 13 and 14 focus on attribution and responsibility. In well-established rules of the law of state responsibility, the conduct of state organs and private actors who are authorised by or operate under the control of the state is attributable to that state and may result in its international responsibility.[27] In their answers to questions 12 and 14, the authors accept these rules and stress the practical difficulties in determining attributability in cyberspace.

Interestingly, in question 12 they hold that the use of the territory of a third state for conducting a cyber operation, which qualifies as an unlawful use of force, may be attributed to the third state, but "with no responsibility for aggression attached."[28] Stated so categorically, this is a highly problematic assertion. First, the mere fact that a state uses the cyber infrastructure of a third state for an unlawful operation against another state hardly suffices for attribution of the cyber operation to the third state. The latter may violate its international obligations by knowingly allowing its territory to be used for activities that result in serious damage in the target state or become internationally responsible for having assisted in the operation, but direct attribution of the conduct of a foreign state as asserted by the authors has no basis in contemporary international law.

Second, their distinction between attribution of the use of force and responsibility for aggression is difficult to understand. If a use of force, which qualifies as an act of aggression, can be attributed to a state, that state will be responsible for the act of aggression unless it can rely on circumstances precluding wrongfulness, such as the right of collective self-defence. It is, of course, possible to distinguish between a use of force and an armed attack, but if a use of force is sufficiently grave to qualify as an armed attack, and if it can be attributed to the third state, the victim state's right of self-defence would not be limited to the primary attacker.

26 *Tallinn Manual*, *supra* note 3, p. 252 *et seq.*

27 International Law Commission, Responsibility of States for Internationally Wrongful Acts, Annex to UN GA Resolution of 28 January 2002, UN Doc. A/RES/56/83, Articles 4, 5 and 8.

28 *Supra* note 2, p. 69.

The responsibility of third states is also addressed in question 13, which deals with the situation of a third state allowing its cyber infrastructure to be used for "unlawful purposes". The authors take the view that it is necessary to "elaborate international legal norms enshrining state obligation not to allow for its national segment of information space to be used for computer attacks against third parties."[29] It would be more than a little surprising if the authors were unaware of the *Corfu Channel* judgment, according to which a state is obliged "not to allow knowingly its territory to be used for acts contrary to the rights of other States."[30] The question arises as to whether they nevertheless advocate new rules of international law for cyberspace, since they seem to be dissatisfied with the existing rules. While the characteristics of cyberspace undoubtedly present new problems, in particular with regard to identification and attribution, this alone does not justify a plea for rules that are stricter than those that are well established. On the contrary, only a comparatively small number of states, probably including the Russian Federation, have the technological capability to influence and monitor the traffic of data that would enable compliance with their proposed international legal norm. For the vast majority of states, stricter standards than those set out in the *Corfu Channel* formula would simply be unacceptable.

State Sovereignty

The issue of whether a cyber operation qualifies as a violation of state sovereignty is addressed in question 18. In particular, the authors query whether "unauthorized access to the e-mail of a state leader or top-ranking official [can be considered] as interference in the internal affairs of a state" or as "a threat to international peace and security, act of aggression, and violation of a state sovereignty." [31] The authors believe that an "unlawful use of ICTs falls under this classification only if it is a socially dangerous action inflicting serious consequences nationally and internationally."[32]

The question combines different concepts of international law that should be dealt with separately. Not every violation of sovereignty or interference in domestic affairs qualifies as a threat to international peace and security or an act of aggression. While an act of aggression is a threat to international peace and

29 *Ibid.*, p. 70.

30 Corfu Channel (U.K. v. Alb.), 1949 I.C.J. 4, at 22 (Apr. 9).

31 *Supra* note 2, p. 70.

32 *Ibid.*

security, the latter concept is not limited to such acts. It is considerably wider and subject to the discretion of the UN Security Council. Furthermore, a cyber operation may indeed be considered a violation of the target state's sovereignty, even if it does not result in the grave or serious consequences considered necessary by the authors. Unauthorised access to the email account of a foreign leader is an act of espionage that is not prohibited by international law. However, a cyber operation that results in the usurpation of functions that belong to the core sovereign rights of the target state may well be a violation of that state's sovereignty, even when it has no serious national or international consequences. Finally, it suffices for the operation to result in either national or international consequences. There is no need for cumulative effects.

Question 19 seems to be closely related to the principle of sovereignty.

> "19. Which international or national institutions are authorized to assess the threats arising from the unlawful use of ICTs for the purposes inconsistent with international peace and security as well as the consequences for security of an individual state in terms of the violation of its sovereignty, territorial integrity and political independence? What criteria should these institutions be guided by?"

Answer:

> "Proceeding from the assumption that international legislation is enforced, in the first instance, by states, there is a concern that the consequences can be miscalculated posing a threat to international security."

One can only speculate about the meaning of the question and the answer. Unless the UN Security Council uses its powers under Chapter VII of the Charter, it is, of course, the right of every state to determine whether there is a threat to, or a violation of, its territorial integrity or political independence. That assessment is always difficult and entails the probability of misinterpretation, which may eventually result in a threat to international security. It is, therefore, hard to see the value added by the question and the answer. The authors could have been more specific by, for example, pointing out the difficulties that exist when it comes to the identification of a cyber attack's source, and the effects it might have on the target state.

Critical Infrastructure

An important issue is the subject of question 23 – critical information infrastructure and its protection against unlawful interference. The authors refer to SCADA and other systems that are crucial for the operation of, *inter alia*,

nuclear and hydroelectric plants.[33] They propose a "formalised" prohibition of attacks against such critical information infrastructure, which could be achieved only following agreement on the criteria that are necessary for inclusion in that category. They believe that the necessary agreement cannot be reached quickly or easily and thus recommend a gradual approach by protecting, as an initial measure, the banking infrastructure.

Naturally, all states that are dependent upon critical information infrastructure are concerned about its vulnerability. They are therefore increasing their efforts to enhance its resilience and protection. Still, it is far from settled whether a "formalisation" of the protection of critical information infrastructure is either feasible or a step into the right direction. First, states have already identified the vulnerabilities of prospective adversaries and many have the means available, including cyber means, to neutralise or interfere with that critical cyber infrastructure if they deem it lawful and necessary. Second, states will not agree on a prohibition of attacks against such infrastructure unless it is universally accepted and accompanied by a well-elaborated verification regime. Third, a verification regime is infeasible because it is almost impossible to distinguish between "innocent" and potentially malicious cyber means. Finally, the invitation to enter into an international agreement on the prohibition of attacks against critical information infrastructure might be a poisoned chalice, the acceptance of which merits thorough consideration.

Human Rights

In conformity with the approach by the UN Group of Governmental Experts, in question 22, the authors consider it necessary to "elaborate norms referring to the protection of human rights and data in information space."[34] They explicitly refer to the human rights recognised in the International Covenant on Civil and Political Rights, without omitting restrictions that may be necessary for the protection of other human rights or of national security, public order, public health or morals. In view of the human rights situation in many countries, the emphasis on possible restrictions of the freedom of information should be regarded with a considerable degree of suspicion. All too often, states have accepted human rights obligations only to subsequently pay them little more than lip service.

33 *Ibid*., p. 73.

34 *Supra* note 2, p. 72

Concluding Remarks

If the article by Andrey Krutskikh and Anatoly Streltsov reflects an official or semi-official position of the Russian Federation on the international legal aspects of cyber security, it should be taken into due consideration by those working in this field, be they government officials, academics or those interested in the subject for other reasons. The Russian Federation is, and will continue to be, a key player in international relations and, thus, in all matters concerning international security, including cyber security. Since the article highlights those issues that seem to be considered important by the Russian Federation, it is a welcome contribution to the on-going international discourse on the international legal implications for cyber security.

At the same time, many of the positions and proposals set forth in the article invite considerable criticism. While certain positions might appeal to some as reasonable or even necessary, all too often they seem to be guided by the intent to use international law as a tool to counterbalance technological inferiority or to increase state control over activities in cyberspace. Modifying and interpreting international law in the way proposed in the article would most probably serve Russian interests, but not necessarily those of other states. The rules and principles of international law, including the *jus ad bellum* and the *jus in bello*, as they stand today should not be altered or subjected to interpretations that have the potential of shattering international legal stability.