CYBER TREATY IS COMING: *Что делать?*

Tikk & Kerttunen (2018)

Stronger and more concerted efforts are needed to shape the international cyber security dialogue to the like-minded advantage. Absent decisive turn in the discourse, the West needs to be prepared for negotiations.

Introduction

The endurance of the Russian international cyber policy has been remarkable. Where the West has had difficulties to advance, Moscow, together with Beijing, have captured new terrain in the past year. This is significant as the western-led 'cyber norms' campaign can be regarded as feeding an even broader community of treaty-minded.

This paper will expose the continuity and appeal of the Russian call for an international agreement. On the one hand, a treaty has always been regarded as a promise of more control over information and the Internet. On the other hand, it increasingly appears as the only way to deliver predictability and certainty to international cyber affairs.

The West needs to anticipate further pressure towards a treaty. To effectively counter-balance the Russian moves, the like-minded need to create credible and actionable support to their incantations for a free, open and secure cyberspace.[1]

Objective Reality[2]

With eyes turned towards the US and China as the powerhouses of economic and technological development, Russia is often regarded as a lesser force in international cyber security. Dealings with Russia have alternated between next to uncritical engagement and all-aggressive reactionary behaviour. Especially since the annexation of Crimea, the West has outright rejected any openings coming from Moscow. Exchanges with Russian scholars and professionals have been deliberately limited.[3] Critical analysis of Russian strategy is scarce.[4]

In treating Russia as the usual suspect, it easily goes unnoticed how, twenty years after first alarming the international community of the threat that information and communication technologies (ICTs) could pose to international peace and security, Russia can demonstrate considerable sympathy to their basic plea.

Russia has built a solid partnership with China, gained support from BRICS, the Collective Security Treaty Organization (CSTO), and the Shanghai Cooperation Organization (SCO) as well as considerable attention from the developing countries.[5] The Moscow-initiated

[1] The paper deliberately remains focused on structural and procedural questions. While highlighting the endurance and coherence of the Russian information security policy and at the same time being critical to and skeptical of the like-minded maneuvers, our argumentation and conclusions do not endorse the direction or content of the Russian policy.

[2] The expression of 'objective realities' refers to a common Leninist, and Russian, argumentation based on undisputable, material facts (leading to one and only one conclusion). See for example V.I. Lenin (1908). *Materialism and Empirio-Criticism. Critical Comments on a Reactionary Philosophy*, Chapter 2:4: "Does objective truth exist?", in *Lenin Collected Works* (1972). Putin administration often refers to the lack of facts in Western accusations of Russian influence or network operations. Moreover, in Soviet political and military operations changing the reality by aggressive maneuver was a common practice.

[3] Georgetown University's annual International Conference on Cyber Engagement is a notable exception among western cybersecurity conferences and workshops that features Russian speakers. Western governments have abstained from the Russian flagship information security conference in Garmisch-Partenkirchen, Germany. In 2015, the NATO Cooperative Cyber Defence Centre of Excellence rejected the participation of Russian nationals at its annual conference, with reference to Excellence denied participation at their annual conference to Russian nationals with reference to NATO Foreign Ministers' Statement of April 1, 2014 (https://www.nato.int/cps/ua/natohq/news_108501.htm).

[4] Notable exceptions include A. Soldatov (2014). Why We Should Care About Russia's Stance on the Internet", *Cyber Dialogue 2014,* MUNK School of Global Affairs, The University of Toronto; A. Soldatov & I. Borogan (2015). "How Putin Tried to Control the Internet", https://motherboard.vice.com; and J. Kukkola, M. Ristolainen & J-P Nikkarila (2017). *Game Changer: Structural transformation of cyberspace*, Finnish Defence Research Agency, No. 10.

[5] For example, the VII BRICS Summit Ufa Declaration (Ufa, the Russian Federation, 9 July 2015) concluded that "the use and development of ICTs through international cooperation and universally accepted norms and principles of international law is of paramount importance in order to ensure a peaceful, secure and

resolution [6] in the UN First Committee has been sponsored by next to 120 states. It has triggered an exchange, between more than 70 countries, of national views and positions on international cyber security.[7] Furthermore, the Russian sentiments can be read in western scholarship and corporate initiatives.[8] Moreover, the once clear separating line that the US had drawn between Internet Governance and international cyber security, is erased with the emergence of cybersecurity governance sub-discourse.[9]

This pincer movement provides a gathering of otherwise hardly compatible groups and views. For many, the appeal of a convention is not the one of control over information. It is, increasingly, the needed predictability and certainty only rules can provide.

Russian information security policy is tailored to national interests and long-term strategy. President Putin, Minister Lavrov and Ambassador-at-Large Krutskikh have achieved an admirable alignment of Russian internal and foreign information security aspirations. The Russian configuration of technological independence, political controls and normative guarantees represents an ideal of national strategy and international policy coherence many states have not been able to achieve.

Moreover, while Russian international information security policy targets Western cyber capabilities, Moscow continues to develop and employ advanced electronic warfare capabilities outside of any international attention and normative considerations.[10] The Kremlin has thus been able to question and compromise the one aspect in the use of ICTs the West promotes and Russia is least interested in developing.

In sum, Russia has not just maintained, but developed and strengthened their call for an *international information security system*. [11] Moscow has been persistent and successful in soliciting support to its main claim and proposed measures. The recruitment of CIS, SCO and BRICS all testify of an ever-solidifying move towards technical, legal and political autonomy in cyberspace.[12]

Meanwhile, the West has not been able to convince and engage states outside its perimeter. [13] Most importantly, the West has been unable to demonstrate the authority of existing international law. The western scholarship, especially within the international cyber security discourse, has remained short of methodology, evidence and clear argumentation. Instead, it has created a plethora of ideas and mini-agendas that outsiders find hard to follow and relate to.

Whereas Moscow and Beijing are largely immune to western accusations of cyber attacks and espionage, the normative authority of the like-minded has been affected by leaks of foreign espionage, mass surveillance and especially the government expectation of corporate assistance in their efforts. Especially the continuing trend of securitizing ICTs

open digital and Internet space". On 23 December 2014 the CSTO member states signed "The protocol of cooperation between CSTO members on countering criminal activity in the information sphere". On 16 June 2009, the Shanghai Cooperation Organization members signed "The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security".

[6] UN General Assembly (1999) Resolution Adopted by the General Assembly, Developments in the field of information and telecommunications in the context of international security, UN Doc. A/RES/53/70.

[7] E. Tikk & M. Kerttunen (2017). "The Alleged Demise of the UN GGE: An Autopsy and Eulogy", Cyber Policy Institute.

[8] See in particular, B. Smith (2017). "The need for a Digital Geneva Convention" (14 February).

[9] On the cyber security – internet governance nexus, see the commentary and summaries of IGF 2017; and Georgia Tech School of Public Policy Internet Governance Project, "What is Internet Governance", www.internetgovernance.org. See also Ridout, T.A. 2016. Here We Go Again: A Comparative Approach to Developing an International Cyberspace Governance Framework.

[10] On Russian EW capacity, see R.N. McDermott (2017). "Russia's Electronic Warfare Capabilities to 2025: Challenging NATO in the Electromagnetic Spectrum". International Center for Defense and Security, Tallinn.

[11] I. N. Dylevsky *et.al.* (2007). "The Military Policy of the Russian Federation in the Field of the International Information Security: Regional Aspect", *Voennaia mysl'*, No. 2; Ministry of Foreign Affairs of the Russian Federation (RU MFA) (2013). "Basic principles for State Policy of the Russian Federation in the field of International Information Security to 2020"; I.N. Dylevsky *et.al.* (2015). "Political and Military Aspects of the Russian Federation's State Policy on International Information Security", *Military Thought*, Volume 24:1; RU MFA (2017). "Statement of the Deputy Secretary of the Security Council of the Russian Federation Oleg Khramov at the international OSCE conference on cybersecurity", Vienna (3 November).

[12] J. Kukkola, M. Ristolainen & J-P Nikkarila (2017). *Game Changer: Structural transformation of cyberspace*, Finnish Defence Research Agency, No. 10.

[13] Although the 2017 Global Conference on Cyberspace (The London Process) was hosted in New Delhi, India (and Pakistan) joined the Shanghai Cooperation Organization in 2016, thereby linking her regional economic and security aspirations with Russia and China.

has prevented the western democracies to gain full coherence of national approaches.

Кто кого?[14]

The west has put an enormous effort into arguing that there is no need for new international law. The US, UK, Canada and Australia all have been unyielding in their national positions.[15] Other like-minded have put forward strong arguments for international rule of law.[16] *The London Process* has offered a number of openings: proposals for principles governing behaviour in cyberspace[17], a call for applying offline laws and norms online[18], the reiteration of the UN GGE findings[19], discussion of legitimate responses available when breaches of international law occur, as well as a strong agenda for taking norm development forward[20]. *The Hague Process* has undertaken to export a western reading of international law. A further Dutch initiative is determined to carry on the norms discourse, a diversion to the international law negotiations made during the 2014/15 GGE. Rather than strengthening the main message, however, the many efforts appear to be fragmenting it.

Doubts about the applicability of existing international law, in the context of cyber threats, are being expressed by western scholars and major western companies. For example, Hollis's duty to hack, e-SOS and the concept of International Law of Information Operations all highlight the lack of legal certainty and underscore the potential of international law.[21] Despite advertised to the contrary, the *Tallinn Manual* points out inconsistencies in law and legal scholarship.[22] This scholarship confirms that alternative reading of international law is possible. Although for cynical operators and policy-makers this provides convenient ambiguity, it also underscores the lack of certainty, predictability and stability.

Roberts's analysis confirms that different approaches to international law are not only possible but also real.[23] Cultivating only the relatively small 'cyber' community does not support the Western goal of broadening common understandings about international law and standards of responsible state behaviour. Elitism in the 'international cyber security' discourse erodes views among the presumably like-minded.

The 'norms' turn, initially seen as a successful western counter-claim to the treaty proposition, has drawn additional attention to the perceived gaps in international law.[24] On the one hand, the norms discourse directly points to inconsistencies in, or about, international law.[25] On the other hand, the artificial and insufficiently clarified separation between 'norms' and international has alerted scholars in both IL and IR to review, and examine in detail, the letter of law against the practice of it.[26]

---

[14] Lenin's question, "The whole question is — who will overtake whom?" (Весь вопрос — кто кого опередит?) at the All-Russian Congress of Political Education Departments, in October 1921, pointing to the class struggle but also to the raging civil war between the Bolsheviks and White Russians (V.I. Lenin (1921) in *Lenin Collected Works*, Vol. 33 (1966)). Both Trotsky and Stalin later used the shortened version of the question.

[15] See national annual submissions on information security to the UNGA (UNODA, "Developments in the field of information and telecommunications in the context of international security") as well as national cyber security strategies (CIPedia, National Cyber Security Strategy).

[16] Among them Germany, The Netherlands, Estonia, Switzerland, Finland, South Korea.

[17] London Conference on Cyberspace (2011). "Summary by the Chairman" (1-2 November).

[18] Budapest Conference on Cyberspace (2012). "Summary by the Chairman" (4-5 October).

[19] Seoul Conference on Cyberspace (2013). "Seoul Framework for and Commitment to Open and Secure Cyberspace" (17-18 October).

[20] The Hague Global Conference on Cyberspace (2015). "Chair's Statement" (16-17 April).

[21] D. B. Hollis (2008). "Why States Need an International Law for Information Operations", *Temple University Legal Studies Research Paper No. 2008-43*; (2011) "An e-SOS for Cyberspace", *Harvard International Law Journal, Vol. 52, No. 2*; (2014) "Re-Thinking the Boundaries of Law in Cyberspace: A Duty to Hack?", *Temple University Legal Studies Research Paper No. 2014-16*.

[22] These include *inter alia* the question of data as an object or not, the threshold of armed attack, the allowing interpretation of the plea of necessity, and foreign espionage as coercive or non-coercive practice.

[23] A. Roberts (2017). *Is International Law International?* Oxford University Press.

[24] Eneken Tikk (ed.) (2018). *UN GGE recommendations commentary*, UNODA (forthcoming).

[25] Whereas in the UN GGE some countries were not willing to accept the applicability of the right of self-defence and IHL in the context of state use of ICTs, others were unable to accept, without reservations, the binding nature of due diligence, and the law of state responsibility.

[26] A rich discussion has emerged around the UN GGE 2015 recommendations on voluntary, non-binding norms, rules and principles. See, for example, Osula, A.-M. and Rõigas, H. (eds.). 2016. *International Cyber Norms Legal, Policy & Industry Perspectives.* Tallinn*:* NATO CCD COE Publications; Broeders, D. 2016. *The Public Core of the Internet, An International Agenda for Internet Governance.* Amsterdam: Amsterdam University Press; Charney, S., English, E., Kleiner, A., Malisevic, N., McKay, A., Neutze, J., and Nicolas, P. 2016. *From Articulation to Implementation: Enabling Progress on Cybersecurity Norms.* Microsoft Corporation; Farrell, H. 2015. 'Promoting Norms for Cyberspace', *Cyber Brief, Digital and Cyberspace Policy program.* NY: Council on Foreign

Absent the norms discourse, gaps in international law could be left to the legal community to debate, therefore occurring at a slower and controllable pace and remaining realistic of international law as a discipline. The norms discourse, initially aimed at states, has come to target and involve stakeholders across the spectrum. [27] The unfortunate unclear relationship that, by way of the UN GGE framing, has come to exist between international law and norms, creates unrealistic expectations towards international law – and fuels the claim of international law being impotent. Mead, Higgins and Koh conclude that "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".[28]

An important obstacle to the like-minded plea of existing international law as a platform of international cyber security is the developing countries' hesitance to accept this not due to the differences about the law itself but because of the lack of capacity and the perceived high cost of implementation. For those audiences it is essential to clearly distinguish, and maintain a clear separation between cyber security and international peace and security issues.

In this context, the west needs to attend another emerging merger, the one of Internet governance with international security. It is essential if the like-minded want to keep the issue of international cyber security out of ITU and avoid a return to WCIT 2012 situation. It is also crucial as Internet governance is a topic that could potentially isolate the US.

What is to Be Done?[29]

To effectively push back on the Russian initiative, the West needs to undermine one of the three pillars in the Kremlin's strategy: the general distrust towards ICTs, the insufficiency of existing international law or the existential threat narrative. On the first account, deeply rooted suspicion cannot be argued away. On the second, Russia has been able to strengthen the general perception of legal insecurity, thereby solidifying her own claim. On the third, the like-minded still possess a strong advantage: their experience of transparency, openness, growth and resilience.

It is in the interests of the West to decisively turn the leading narrative from threats to opportunities and emphasize national accountability. The fact that the UN GGE has not been able to establish a real linkage between state use of ICTs and threats to international peace and security, or verify any existential threat linked to ICTs, should encourage a more critical and analytical look at the types of threat that the proliferation and convergence of ICTs actually bring. In this context, too, cyber security should not be mixed with international peace and security issues. To the extent ICTs cannot be concluded to constitute an existential threat, any dialogues in the arms control realm should be strictly limited to development and employment of particular military capabilities.

Relations; Finnemore, M. and Hollis, D. 2016. 'Constructing Norms for Global Cybersecurity', *American Journal of International Law*, 110 (3); Korzak, E. 2016. 'The Quest for Cyber Norms', *Bulletin of the Atomic Scientists*, 72 (5): 348-350; Mačák, K. 2016. 'Is the International Law of Cyber Security in Crisis?', in Pissanidis, N., Rõigas, H. and Veenendaal, M. (eds.) *2016 8th International Conference on Cyber Conflict Cyber Power.* Tallinn: NATO CCD COE Publications; Maurer, T. 2016. 'The New Norms: Global Cyber-Security Protocols Face Challenges', *IHS Jane's Intelligence Review,* March: 52-53; Mazanec, B.M. 2015. 'Why International Order in Cyberspace is Not Inevitable', *Strategic Studies Quarterly*, Summer: 78-98; Tikk-Ringas, E. 2017. 'International Cyber Norms Dialogue as an Exercise of Normative Power', *Georgetown Journal of International Affairs*, *International Engagement on Cyber VI*, Vol. 17, No. 3. See also Soesanto, S. and D'Incau, F. (2017) The UN GGE is dead: Time to fall forward; available at http://www.ecfr.eu/article/commentary_time_to_fall_forward_on_cyber_governance; Melissa Hathaway (2017) When Violating the Agreement Becomes Customary Practice, in Getting beyond Norms: New Approaches to International Cyber Security Challenges, Special Report Centre for International Governance Innovation (CIGI); Liis Vihul and Michael N. Schmitt (2017) International Cyber Law Politicized: The UN GGE's Failure to Advance Cyber Norms, available at https://www.justsecurity.org/42768/international-cyber-law-politicized-gges-failure-advance-cyber-norms/; Adam Segal (2017) The Development of Cyber Norms at the United Nations Ends in Deadlock. Now What? Available at https://www.cfr.org/blog-post/development-cyber-norms-united-nations-ends-deadlock-now-what).

[27] A notable example is the Global Commission on the Stability of Cyberspace (GCSC), co-partnered between Governments of The Netherlands, Singapore and France, Microsoft Corporation and the Internet Society and sponsored by government of Estonia. GCSC seeks to "link the dialogues on international security with the new communities created by cyberspace" in its goal to support "policy and norms coherence related to the security and stability in and of cyberspace". See cyberstability.org.

[28] M. Mead, R. Higgins and H. Koh (2017). "From cyber norms to cyber rules: re-engaging states as law-makers", *Leiden Journal of International Law*, Vol 30(4).

[29] *Что делать?* (Chto delat?), V.I. Lenin (1902). "What Is To Be Done? Burning Questions of Our Movement" in *Lenin Collected Works*, Volume 5 (1961).

The West should avoid countering the Russian narrative as a whole. The discourse needs to mature beyond either-or approaches that toy with the idea of one camp surrendering to the other. The West needs more than merely a friendly or adversarial policy option to successfully counter Russian informational, cyber and normative power projection. One can think of the policy of undermining as a non-confrontational approach and principle that organizes various otherwise individual proactive and reactive measures according to a single, coherent intention and a shared long-term objective. Essentially, undermining would seek to deny, diminish, nullify, turn, change or overwhelm Russian activities, their effects and the support of them. It would be intended to increase the cost of such activities through cyber-specific and other means.

The West is uniquely placed to counter-balance the Russian threat narrative with a progressive initiative. A *Cyber Marshall Plan,* building robust national capacities and unprecedented transfers of ICTs, would effectively undermine the Russian agenda and agitation of fear, insecurity and xenophobia. A determined program launched in the spirit of the original Marshall Plan would honor the ingenious ideal of creating a climate of wealth, health and security. It would also undermine the Russian project to show, through its own active operations, the vulnerability of cyberspace.[30]

The like-minded cannot afford fragmentation and soloing that goes against the acknowledged shared concerns and priorities. For instance, mingling with Internet governance concepts in the context of international cyber security adds strategic weight to the intersection importing governance into the First Committee paradigm. It easily also opens Internet governance to further pressure of state-centric control.[31] In this context, any differences that the like-minded have about and around Internet governance, are easily turned into isolating factors in the international cyber dialogue. Moving forward, the like-minded need to be cognizant of the differences and non-alignment between them and learn to leave these aside in negotiations.

The like-minded must also become more mindful of the potential disadvantages of long-term securitization of ICT matters. Where the civil society, academia and the people's representatives are kept out of the dialogue, exercise of executive power at the verge of legitimacy is likely to incur strong pleas towards transparency and accountability.

Where the dialogue has been diluted to the point of no return, there are options to avoid overwhelming vote count towards an undesired policy direction. A way to square this circle is to bucket the three core interests of security, human rights, and technological development. The buckets could be negotiated separately, and partially within true expert communities, but they would not be agreed or implemented in segregation.

Another way to increase shades-of-grey to cyber discourse is to identify shared national interests and objectives across camps and continents. This would help to build new thematic coalitions with the intention to solve problems outside of the stagnated blocks and opined arguments.

The policy of consequences as a continuation of the discourse of legitimate responses under international law, runs an additional risk of revealing true differences in national understanding, interpretation and implementation of international law. This, at the time of already heightening tensions might prove counterproductive to the rule of law narrative.

Can We Go Forward if We Fear to Advance?[32]

Further pressure towards a treaty is inevitable. As parity with the US is the Russian condition of strategic stability, the Kremlin will keep using the treaty argument to reduce its insecurity. In this effort China and Russia remain aligned. Russia has, or will shortly have, the confidence and collaboration to move towards formal negotiations. The western rejection, 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.

[30] The authors thank Juha Kukkola for this clear remark in his commentary to the draft of this paper.

[31] Entering the UN GGE discussion in 2015, The Netherlands suggested further work and concrete measures to establish special normative protection for certain systems and networks, including certain critical components of the global Internet. See UN A/70/172, page 8.

[32] Paraphrasing Lenin's "Can We Go Forward If We Fear to Advancing Towards Socialism" (V.I. Lenin (1917). The Impending Catastrophe and How to Combat It. *Lenin's Collected Works*, Vol 25).

Western outright rejection would not necessarily prevent negotiations. For instance, drafting and the eventual voting of a UN resolution to negotiate a legally binding instrument to prohibit nuclear weapons split the West, the BRICS, the SCO and the developing countries.[33] A convention can result from further corporate or civil society initiative. For example, the 1997 Anti-Personnel Mine Ban Treaty (the Ottawa Convention) was borne out of civic engagement and NGO movement. [34] It is not unprecedented that a group of countries or a regional organization becomes the platform for a global instrument. The 2001 Convention of Cybercrime (the Budapest Convention) is by origin a European instrument that has gradually gained support from individual countries across the world. [35] Furthermore, a treaty may become a question due to a spillover from a related area or set of questions. For instance, differences about space issues may create the question about similar themes in the context of ICTs, absent *lex specialis*. If Western concerns over Chinese and Russian advancement in quantum computing, artificial intelligence, electronic warfare and lethal autonomous capabilities are correct then eventually it would be in the Western interest to establish a strong treaty-based regime to limit such development and employment.[36]

Should a Sino-Russo initiative for treaty negotiations materialize the West should take the gambit at face value. This would reveal how seriously and how far Moscow and Beijing actually are willing to take and develop international law. By the same token, at least China appears to be interested in not being seen as undermining international law.

To advance, the West needs to prepare for treaty negotiations as one possible future. It is in this context essential to realize the value and potential of independent and constructive national positioning on matters of international law and the development thereof. It is hardly an accident that the 2016/17 GGE featured countries like Switzerland, Finland and South Korea, all of which are regarded as champions of rule of law and potentially accepted as honest brokers in international cyber affairs. Further to this logic, Singapore seems to be emerging as advocate of developing and implementing cyber norms in accordance with ASEAN values.

Preparing for the worst-case scenario, it will be possible to find new openings to avoid it. A square where the West can meet Russia is one of principles for international cyber security. Here, without drowning in the details and modalities of international law, states have space to agree on general directions and the minimum world order.

[33] UNGA (2016). "General and complete disarmament: taking forward multilateral nuclear disarmament negotiations", A/C.1/71/L.41 (14 October). The resolution was sponsored by Austria, Brazil, Chile, Costa Rica, Democratic Republic of the Congo, Ecuador, El Salvador, Guatemala, Honduras, Indonesia, Ireland, Jamaica, Kenya, Liechtenstein, Malawi, Malta, Mexico, Namibia, Nauru, New Zealand, Nigeria, Palau, Panama, Paraguay, Peru, Philippines, Samoa, South Africa, Sri Lanka, Swaziland, Thailand, Uruguay, Venezuela and Zambia.
In the December 2016 UNGA voting Albania, Andorra, Australia, Belgium, Bosnia and Herzegovina, Bulgaria, Canada, Croatia, Czech Republic, Denmark, Estonia, France, Germany, Greece, Hungary, Iceland, Israel, Italy, Japan, Latvia, Lithuania, Luxembourg, Micronesia, Monaco, Montenegro, Norway, Poland, Portugal, Republic of Korea, Romania, the Russian Federation, Serbia, Slovakia, Slovenia, Spain, Turkey, the United Kingdom, and the United States voted against the resolution. Armenia, Belarus, China, Finland, Guyana, India, Kyrgyzstan, Mali, Morocco, the Netherlands, Nicaragua, Pakistan, Sudan, Switzerland, Uzbekistan, and Vanuatu abstained.

[34] UNOG (1997). *Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction*. China, the United States, and Russia did not sign the convention. The US, however, announced in 2014 that it would abide by the terms of the Treaty, with the exception for anti-personnel mines employed on the Korean Peninsula.

[35] Council of Europe (2001).

[36] For recent Western statements on Chinese and Russian capabilities see for example; C. Scaparrotti (2017). "Military Assessment of Russian Activities and Security Challenges in Europe", Committee on Armed Services, United States House of Representatives (28 March); DOD (2017). "Military and Security Developments Involving the People's Republic of China 2017"; DIA (2017). "Russia Military Power"; and W. Carter (2018). "Chinese Advances in Emerging Technologies and their Implications for U.S. National Security", Statement Before the House Armed Services Committee Subcommittee on Emerging Threats and Capabilities (9 January).