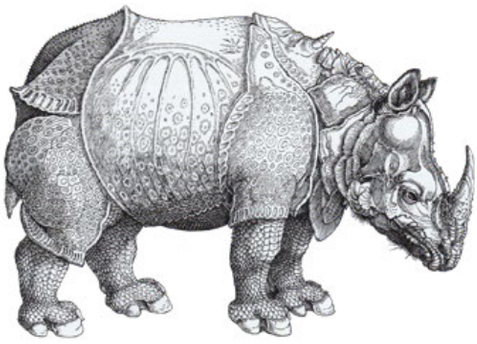

SECURITY INDEX

Occasional Paper Series

№ 4 | 2019

"No Holds Barred" and the New Vulnerability: Are We in for a Re-Run of the Cuban Missile Crisis in Cyberspace?

Vladimir A. Orlov

The paper "'**No Holds Barred' and the New Vulnerability**" addresses the question whether the international community has to survive a cyber equivalent of the Cuban Missile Crisis to realize the importance of achieving some kind of agreement on cyber issues, and on the broader agenda of international information security. Given the recent US Cyber Strategy that emphasizes offensive rather than purely defensive operations against Chinese and Russian military and cyber infrastructure, inaction is no option for Russia. Though there is a considerable degree of scepticism about the possibility of drafting an international convention on non-proliferation of cyber-weapons amid deteriorating security situation, yet a first step must be made, and it does not have to be legally binding or comprehensive.

The article is written by Professor at Moscow State University of International Relations (MGIMO); Founder and Director of PIR Center **Dr. Vladimir A. Orlov**

Read the paper on PIR Center website

Key findings

- **It took the Cuban Missile Crisis in October 1962, and the sudden appearance of Soviet nuclear weapons and missiles in Cuba, for the US leadership to realize that America's nuclear invulnerability was gone, never to return.** It took the Cuban Missile Crisis for everyone to understand that the future of our nations and of the entire planet could not be risked in a game of nuclear brinkmanship. Joint Soviet-US efforts to prevent the spread of nuclear weapons, combined with a bilateral system of nuclear deterrence and arms control architecture, have kept us from sliding towards an abyss.

- **The fear of cyberweapons is not on the same level as the fear of nuclear weapons.** Nevertheless, it is also great, and it continues to grow because there's no way of telling where the next blow may come from. This feeling of new vulnerability is akin to the feeling during the Cuban Missile Crisis. The realization that a potential adversary (a non-state actor or, more likely, a hostile state) may use the invisible IT networks to strike at our nuclear weapons control systems, our personal email boxes, our vote-counting systems, and our critical infrastructure facilities, leaves some paralyzed, others paranoid, and still others determined to prepare a symmetric or asymmetric response to any such attack. An eye for an eye, a tooth for a tooth – even if the eyes and teeth in question exist only in

virtual reality. After all, the line between the virtual and the real is becoming so blurred that we may one day find ourselves, to our horror, eyeless and toothless.

- **The world is sliding to another major crisis like the one in 1962.** The cyber war is already raging. There are no rules of engagement in that war. The uncertainty is high. The spiral of tension is getting out of control. The cyber arms race is gaining momentum. And there are no guarantees that the next crisis will be controllable, or that it will result in a catharsis as far as international information security regulation is concerned.

- **Bilateral agreements between key international infospace actors could become an important interim step towards a comprehensive solution.** But the spiraling crisis in international arms control makes any such bilateral, legally binding agreements on cyber weapons patently unrealistic, at least for the time being. In other words, for the time being, there are no holds barred.

Read the paper on PIR Center website

About the Author

Dr. Vladimir A. Orlov is expert in international security and Russia's foreign policy. Dr. Orlov founded PIR Center, a private think-tank dealing with global security and foreign policy, in 1994. In 2001-2002, the U.N. Secretary-General appointed Dr. Orlov as a U.N. consultant on disarmament and nonproliferation education. Since 2014, Dr. Orlov is the Head of the Center for Global Trends and International Organizations at the Diplomatic Academy in Moscow. Dr. Orlov served as a member of the UN Secretary General's Advisory Board on Disarmament Matters (2015-2019). Since 2017, Dr. Orlov is MGIMO Professor (at Department of Applied Analysis of International Affairs). On October 7, 2019, he was appointed Director of PIR Center by the Center's Executive Board at its annual session.

About

To contents

"Security Index" Occasional Paper Series presents reports, analytical articles, comments and interviews that reflect the positions of Russian and foreign experts on the current challenges of global security and Russian policy in this sphere. The series aims at providing clear analysis of global security problems and suggesting practical solutions.

"Security Index" Occasional Paper Series continues the "Security Index" journal published by PIR Center in 1994 – 2016. Authors and editors will be glad to receive comments, questions and suggestions on our e-mail address inform@pircenter.org.

PIR Center Director: *Vladimir A. Orlov*
Occasional Paper #4 Editor: *Natalia Artemenkova*

Our e-mail address: **inform@pircenter.org**

'NO HOLDS BARRED' AND THE NEW VULNERABILITY: ARE WE IN FOR A RE-RUN OF THE CUBAN MISSILE CRISIS IN CYBERSPACE?

Vladimir Orlov

It was almost two decades ago, when I was brought a manuscript. It was entitled "Information challenges to national and international security". International information security – or cybersecurity, to use the more popular but grossly oversimplified term – is now high on the agenda of global challenges. But back at the time, things were different. It wasn't an obscure issue by any means, but discussions were mostly confined to the expert community, and they were usually overshadowed by more pressing concerns. And then 9/11 happened, whereupon international terrorism eclipsed all other threats for years to come.

As soon as I had a closer look at that manuscript, it became clear to me that this was an extraordinary piece of analysis – and that the magnitude of the global threat it discussed was far greater than I had previously imagined. The paper placed special emphasis on scenarios for cyberwars… I first wanted to write "future cyberwars", but the papers' authors rightly pointed out that those cyberwars were in fact already happening.

The paper warned of the risk of a cyber conflict degenerating into an exchange of nuclear missile strikes. It rightly argued that in a bilateral armed conflict, the response of the party that has been attacked using information weapons is also completely unpredictable. "A situation may arise whereby the party that has come under a very limited attack using information weapons overreacts because it mistakenly believes that the attack it has detected is only the "tip of the iceberg". That overreaction may include a limited or massive use of nuclear weapons."[1]

"At this stage, banning the development and use of information weapons – in the same way that chemical and biological weapons have been banned – does not appear a realistic prospect. It is also clear that it's impossible to limit the efforts by many countries to form an integrated, global information space. That is why any solutions can be found only by reaching reasonable agreements based on international law and aimed at minimizing the threat of information weapons use."[2]

I greenlighted the manuscript's publication – and once released, the paper caused quite a stir. I distinctly remember the hype at the briefing convened specially to announce that publication held at the Russian Foreign Ministry's press center. Indeed, some authors of the paper were from the Foreign

Ministry itself while others were from the Federal Security Service (FSB), Foreign Intelligence Service (SVR), Interior Ministry, and Russian National Security Council, among others.

Naked and Afraid

It has now been 18 years since that day. IT has made unprecedented and unimaginable progress. The Internet has become like oxygen; people would literally suffocate without their daily online fix, and dependence on the online world has become pervasive. Everyone and their dog are now writing about information wars, and *cyber* is a far more popular subject than *nuclear* for graduation papers at international studies schools. For several years now, the UN has hosted discussions on international information security at the Group of Governmental Experts (GGE) on Achievements in Informatization and Telecommunications in the Context of International Security.

To use the name of a popular TV show, ordinary people feel *naked and afraid* before the threats lurking in information space. *Naked* because they lack any protection, and *afraid* because they know it. The fear and bewilderment, which border on panic and paranoia, sometimes have entire countries in their grip.

But despite all that, little has been done to tackle the threat. After all these years, the international community has become no closer to developing the cyber equivalent of the Nuclear Non-Proliferation Treaty, a legally binding *cyberNPT* accord that would shield humanity from information wars. This is simply impossible, some reputable experts insist. Unlike nuclear weapons, they go on, it's often impossible to identify the perpetrator of a cyberattack. Furthermore, it is almost always impossible to tell whether the attacker was a state or a non-state actor.

There are, however, some equally reputable experts who counter that there's nothing impossible about it. Natalia **Kaspersky**, head of InfoWatch Group, has proposed "drafting an international convention on non-proliferation of cyber-weapons and the recognition of non-proliferation of cyber-weapons by all countries. It is necessary… to strive to ensure that all countries, especially the leading powers, sign such a convention»[3].

As a compromise and/or an initial step to preventing a *cyber bloodbath*, some are proposing international "codes of conduct" in cyberspace. The latest example is the Paris Call to Trust and Security in Cyberspace, an initiative proposed in November 2018 by the French president. Other examples include proposals on international cybersecurity rules put forward by Microsoft in 2014 at the Global Cyberspace Cooperation summit in Berlin.[4]

Clearly, a first step must be made - but it does not have to be legally binding or comprehensive. It is, however, important to make sure right from the start that every country's and every region's interests and views are taken into account. Confidence-building measures and codes of conduct share a major weakness: they tend to be amorphous and impossible to verify, and compliance is not compulsory. The strength of the NPT – a major treaty that has become a cornerstone of global security – is that it's nearly universal and counts 192 states among its members. The global nature of information threats requires a global response, a treaty that is as universal and respected as the NPT has become in its own sphere.

In these circumstances, bilateral agreements between key international infospace actors could become an important interim step towards a comprehensive solution. But the spiraling crisis in international arms control makes any such bilateral, legally binding agreements on the information sphere (or, not to beat about the bush, on cyber weapons) patently unrealistic, at least for the time being. In other words, for the time being, there are no holds barred.

And when no holds are barred, some tend to lose their head and go too far, because power corrupts. Governments and experts had their suspicions about the true scale of US operations in cyberspace – but the facts disclosed by Edward **Snowden** in June 2013 turned those suspicions into certainty. The degree of US meddling in cyberspace all over the world has been unprecedented. The US state-sponsored information attacks are mostly targeted against a handful of states whose sovereignty is not a mere formality, and who dare to pursue an independent foreign-policy course. Washington has repeatedly – and largely successfully – used cyberweapons against Iran, including against the country's peaceful nuclear infrastructure[5].

But the main target of US information and cyberattacks is not Iran. It is Russia. As the Kremlin concluded in February 2019, "[the] U.S. territory is constantly being used to organize a huge number of cyber attacks against various Russian organizations. That's the reality with which we live"[6]. As a the headline of an article in a recent issues of the reputable Bulletin of the Atomic Scientists put it: "Cyberattacks on Russia - the nation with the most nuclear weapons - pose a global threat"[7]. For the Russian Federation, its own cyber vulnerability has already been put into stark relief.

A new vulnerability

Last summer, my wife and I escaped from New York, Washington, and Chicago into the Midwest, Route 66, and more, crossing 6,000 miles and 19 states. I can write volumes about this epic trip; and I will. But for the purpose of this

article I can summarize my impressions in one sentence: I have found no hatred of Russia and the Russians among ordinary Americans. Full stop. Throughout my trip, I met remarkably welcoming, hospitable people, either Russia-neutral, or Russia-positive, or Russia-curious, people who were always ready to help and eager to learn more. And, only when we were sitting and chatting with a beer or two in a local pub, somewhere in Oklahoma or Wyoming, and the TV was on, not on soccer World Cup but on the news, people started joking: "Will I be investigated for talking to a Russian?" (and always adding: "I don't care"). A saw no Russophobia in the American heartland – but I surely sensed the feeling of vulnerability. In that regard, there is little difference between rural America and Washington, although the feeling is of course more palpable in the US capital. And why is that?

On July 16, 1945, the United States acquired a monopoly on nuclear weapons after testing an atomic bomb – the so-called Trinity Test – at Alamogordo. But Washington retained that feeling of monopoly and impunity even after the Soviet Union conducted its own nuclear test on August 29, 1949. American nuclear-weapons exceptionalism was undermined, but the disparity between the US and Soviet nuclear arsenals remained so large (and not in Russia's favor of course) that the United States continued to feel invulnerable. Even when the Soviet Union began to reduce the nuclear-weapons gap, even when it began to improve the accuracy and range of its missile delivery systems, and even when it tested the hydrogen *Tsar Bomba* at the Novaya Zemlya range on October 30, 1961, Washington did not begin to perceive Moscow as an equal in the nuclear race. It still had the full confidence and the feeling of absolute security.

It took the Cuban Missile Crisis in October 1962, and the sudden appearance of Soviet nuclear weapons and missiles in Cuba, in America's underbelly, for the US leadership to realize that the world had changed. They finally saw that America's nuclear invulnerability was gone, never to return. Let us give credit here to JFK: reading the minutes of his meetings in the White House during the Cuban Missile Crisis[8], you can see him rapidly maturing, comprehending the situation, and – once the full scope of the crisis had been realized – keeping his ministers and advisors from sliding towards a nuclear war. You can see him finding an inner strength to seek a compromise. Incidentally, he did that despite the enormous domestic pressure, despite the calls to be "tough on Russians" and "respond with the full military might", because the crisis was unfolding in the run-up to mid-term Congressional elections.

The lessons of the Cuban Missile Crisis were well-learnt. Only nine months later, the Soviet Union and the United States put their signatures on the Partial Nuclear Test Ban Treaty, which banned nuclear tests in the atmosphere, outer

space, and under water. The draft of that treaty had been languishing for a few years on the negotiating table; both sides would always find a pretext for not signing because there was no political will at the very top. Work soon began on the Nuclear Non-Proliferation Treaty; that work did not stop even after the assassination of JFK. It took the Cuban Missile Crisis for everyone to understand that the future of our nations and of the entire planet could not be risked in a game of nuclear brinkmanship. Joint Soviet-US efforts to prevent the spread of nuclear weapons, combined with a bilateral system of nuclear deterrence and arms control architecture, have kept us from sliding towards an abyss.

Of course, one cannot simply ignore the vastly different nature of nuclear weapons and cyberweapons. As the former secretary of the Russian National Security Council and ex-Foreign Minister Igor Ivanov recently put it, "nuclear weapons were created and deployed to deter potential adversaries rather than for immediate use. The fear of a global nuclear war presupposed maximum caution and high responsibility of nuclear powers. The situation is different with cyber weapons, — today few people believe that their use creates an immediate threat to all of humanity. Therefore, the temptation to use this weapon might be too great. While cyber weapons are largely anonymous, a cyberattack can be launched from almost anywhere on the planet, and the real cyber aggressor may remain unidentified, and therefore unpunished."[9]

The fear of cyberweapons is not on the same level as the fear of nuclear weapons. Nevertheless, it is also great, it continues to grow, and it's all the more poignant for the fact that there's no way of telling where the next blow may come from.

This feeling of new vulnerability, the realization that a potential adversary (a non-state actor or, more likely, a hostile state) may use the invisible IT networks to strike at our nuclear weapons control systems, our personal email boxes, our vote-counting systems, and our critical infrastructure facilities[10] - that feeling leaves some paralyzed, others paranoid, and still others determined to prepare a symmetric or asymmetric response to any such attack. An eye for an eye, a tooth for a tooth – even if the eyes and teeth in question exist only in virtual reality. After all, the line between the virtual and the real is becoming so blurred that we may one day find ourselves, to our horror, eyeless and toothless.

It is that feeling of new vulnerability - which is akin to the feeling during the Cuban Missile Crisis, when everyone in America thought Soviet missiles were pointed at them from Cuba – it is that feeling that I increasingly sense in Washington and beyond.

I do not wish to speculate about what happened - or did not happen – in 2016 during the US presidential race. It is clear to me that the American voters made their choice based on their own convictions, and not under any "external" pressure. Those who believe otherwise simply lack respect for their own people, thinking them so pliable to external manipulation.

Speaking more generally, the *Russian threat* and the *Russian meddling* are nothing more than an excuse for many in Washington to get even with their domestic political opponents. The polarization of the US elites has gone so far that anything goes in such a brawl. Russia is merely a convenient instrument for US politicians to beat each other over the head. But there is also real wariness of Russia. The reason for that wariness is much deeper than simply trying to establish whether the Russian state really did meddle in US elections. The real reason is that feeling of new vulnerability: even If Russia had not meddled… it could have, it had the ability… which it might well use in the future.

This feeling of new vulnerability requires some response… Here is where the sanctions come on the scene, as a convenient and a long-trusted tool. But sanctions are a poor shield against cyberwars. In fact, they are more likely to fan the flames.

At war

The war is already raging – or have you not noticed? It's no wonder if you haven't. Because the war is mostly invisible, just like any proper cyberwar is supposed to be.[11] Russian experts have drawn a list of distinctive characteristics of such a war. In particular, they highlighted the extreme complexity of tactical warning and damage assessment: "There is a real risk that the damage assessment for specific attacks and situations provided to the national military-political leadership by the various law-enforcement agencies and intelligence services may prove conflicting and contradictory. The attacker can use information weapons to wage strategic operations with unprecedented speed, and instantaneously withdraw to its home cyberspace once the goals of the attack have been achieved."[12]

It was already almost two decades ago when Russian governmental experts suggested that the mass media were the most effective conduit for operations aimed at destabilizing the adversary. The instruments of achieving an impact via the media, in their view, may vary. They may include impact on the infrastructure of the media outlets; impact through the adversary's media; if that is impossible (or to achieve a greater effect), alternative channels of information and psychological impact can be created (such as alternative media outlets, foreign broadcasts, online sources); impact on the adversary

state's political leadership and public opinion, or creating an international climate that makes it more difficult for the adversary to achieve its objectives[13].

Amid America's bloodthirsty domestic politics, any dialogue on cyber issues has become problematic. "Rosy prospects for the normalization of Russian-US ties are not visible on the horizon," said Russian presidential spokesman Dmitry **Peskov** in November 2018 – and he's certainly in a position to know as, in addition to his main functions, he is directly involved in shaping Russia's policy towards the US.[14] Unsurprisingly, quite a number of US experts believe that eventual Russian use of cyberweapons against the United States is inevitable – on the "eye for an eye" principle, as a retaliatory rather than preemptive strike. It is clear to them that Russia is capable of effective, comprehensive, and asymmetric action in the information space. But unlike a nuclear war, a cyber war can involve hundreds of thousands of unseen exchanges of strikes. Only a few of them will be aimed at military targets; the vast majority will exploit political and psychological vulnerabilities.

With war looming large on the horizon, America's largest IT corporations are already preparing. Many have set up war rooms. Facebook, which also owns Instagram and WhatsApp, is among the leaders in that regard. Its war room does not have any windows (I mean physical ones), and it is manned by twenty experts in combating "fake penetration". The number should eventually rise to 20,000. As Mark **Zuckerberg** said in his congressional testimony, "we were too slow to spot this type of [Russian] information operations interference. Since then, we've made important changes to prevent bad actors"[15]. According to the head of Facebook's cybersecurity policy, "Our job is to detect ... anyone trying to manipulate the public debate. We work to find and remove these actors."[16]

In the cyber war-related domain, the United States has been collaborating closely with their closest allies, most notably, with the United Kingdom, particularly, through the Five Eyes agreements on cyber data sharing and coordination of actions. Alex **Younger**, the MI6 chief, also known as "C", in his rear public address in December 2018 at St. Andrews University in Scotland, presented the world as one of liberal democracies fighting for order against an unnamed "skilled opponent unrestrained by any notion of law or morality." He recognized that, as a result, Cyber turned into the MI6's "fastest-growing directorate"[17].

A re-run of the Cuban Missile Crisis in cyberspace?

Meanwhile, time for dialogue is running out. The American "no holds barred" approach has already run into serious opposition, and not only from Russia but

also from China[18], America's key strategic partner/rival in global affairs. Unfortunately, even that has failed to convince Washington of the *pressing need* to talk.

To the contrary: the recently adopted US Cyber Strategy emphasizes offensive rather than purely defensive operations against Chinese and Russian military and cyber infrastructure. This is what the leading US specialists who have served in key cyber posts in the Pentagon have to recommend these days: "The U.S. could remotely target Russia's military command-and-control infrastructure with malware or implant malware through human-enabled close access. Potentially, the U.S. could shut off power around Russian military bases responsible for cyberspace activities, or partner with private-sector players to kick the Russians off private networks and shut off elements of the Russian internet."[19]

Under these circumstances, inaction is no option for Russia. As Director of the Russian Foreign Intelligence Sergey **Naryshkin** recently put it, "haunted by the shadows of the past, the United States are becoming more like Goliath, the presumptuous Biblical giant who, as you know, was defeated by young David…. It's important to stop the reckless game of whose stakes are higher and give up power projection in state-to-state relations, so as not to bring the situation to a new Cuban missile crisis."[20]

As part of its preparations for the July 2018 **Putin – Trump** summit in Helsinki, Russian team drafted a joint presidential statement. Item three of that statement, on the very first page (immediately after the paragraphs on strategic stability, nonproliferation, and terrorism) called for the relevant Russian and US government agencies "to maintain and deepen their discussions on illegal activities in cyberspace, as well as for joint and parallel measures to prevent any destabilizing impact on critical infrastructure and domestic political processes, including elections, in our two countries".[21]

Instead, the two presidents failed to issue any joint statement in Helsinki. Moreover, they failed to address the cyber issue at all, neither in Helsinki nor later last year, as they failed to schedule any meaningful *tete-a-tete* in Paris or Buenos Aires where they both were present at the same time.

Not hundred per cent of the dialogue has been frozen, fortunately. Certain informal, mostly off-the-record, meetings of US and Russian experts on cyber agenda continue taking place, both through Track 2 and Track 1.5. One of the most intellectually stimulating meetings, with frank exchanges, took place in Vienna in December 2018. The report produced after the meeting stressed "the significant risk […] that cyber-attacks could conceivably lead to a military escalation that may further trigger a nuclear weapons exchange, a fact that became more explicit with the adoption of the current Nuclear Posture Review.

This issue gets complicated given that third parties may have the capabilities to invoke a cyber conflict between Russia and the United States. Whether a country or a non-state actor, they could put the two countries on the verge of an armed conflict by attacking critical infrastructure of either of them and making it look as if the aggressor were the other one"[22]. However, one should have no illusion: such informal meetings may be fully fruitful only when their reports and policy recommendations are utilized by the governments. And for that, a warmer climate in bilateral relations is a must. So far, we see exactly the opposite: mercury falling to freezing levels.

Risk of cyber clashes growing into a chaotic global cyber war has been emphasized by the UN Secretary-General Antonio **Guterres** in his Agenda for Disarmament: "Malicious acts in cyberspace are contributing to diminishing trust among States… States should implement the recommendations elaborated under the auspices of the General Assembly, which aim at building international confidence and greater responsibility in the use of cyberspace. [23]" However, as the members of the US-Russian Track 1.5 working group on strategic stability recently concluded, "without a constructive dialogue on cyber issues between the United States and Russia, the world would most likely fail to agree on any norms of responsible behavior of states in cyber space"[24].

Do we really have to survive a cyber equivalent of the Cuban Missile Crisis to realize the importance of achieving some kind of agreement on cyber issues, and on the broader agenda of international information security?[25] Or is that kind of talk plain old alarmism?

I don't want to sound a fatalist, but I am even less keen on sounding like an ostrich that's buried its head in the sand. We cannot ignore the obvious: whether the world's most powerful actors like it or not, the world is sliding to another major crisis like the one in 1962. The cyber war is already raging. There are no rules of engagement in that war. The uncertainty is high. The spiral of tension is getting out of control. The cyber arms race is gaining momentum. And there are no guarantees that the next crisis will be controllable, or that it will result in a catharsis as far as international information security regulation is concerned. There's no telling what will happen once the cyber genie is out of the bottle.

And that is why I fear we're all in for some real – rather than *fake* – drama in cyberspace.

An earlier version of this article was published, in Russian language, in Rossiya v Globalnoy Politike (Russia in Global Affairs) magazine, and its conclusions

were presented at the Track 1.5 meeting of the US-Russian working group on strategic stability in Vienna in December 2018.

[1] Alexander Fedorov and Vitaly Tsygichko, Editors. Information challenges to national and international security. Moscow: PIR Center, 2001. p.94-95
[2] Alexander Fedorov and Vitaly Tsygichko, Editors. Information challenges to national and international security. M.: PIR Center, 2001. p.198-199.
[3] 2017 Moscow Conference on International Security. Conference Proceedings, Speech of Natalya Kaspersky, p. 98 http://www.pircenter.org/blog/view/id/355
[4] For the list of proposed cybernorms, see: http://aka.ms/cybernorms
[5] See: Oleg Demidov. Global Internet Governance and International Security in the Field of ICT Use. Moscow - Geneva, 2015, pp.29-32.
[6] Polina Nikolskaya, Katya Golubkova. Kremlin says cyber attacks on Russia often launched from U.S. territory. February 27, 2019. https://www.reuters.com/article/us-usa-trump-russia-kremlin/kremlin-says-cyber-attacks-on-russia-often-launched-from-u-s-territory-idUSKCN1QG183?il=0
[7] Ramana M. V. & Mariia Kurando (2019). Cyberattacks on Russia - the nation with the most nuclear weapons - pose a global threat. Bulletin of the Atomic Scientists, 75:1, pp.44-50.
[8] See: The Kennedy tapes: inside the White House during the Cuban missile crisis. Harvard University Press, 1998.
[9] Igor Ivanov: "International Security and "Turbid Waters" of Cyberspace", RIAC, January 29, 2018 http://russiancouncil.ru/en/analytics-and-comments/analytics/international-security-and-turbid-waters-of-cyberspace/
[10] For more on cyber threats to civilian nuclear infrastructure, see my paper released ahead of the World Economic Forum: Vladimir Orlov. Our nuclear facilities are increasingly vulnerable to cyber threats. This is what policy makers need to know. October 5, 2016 https://www.weforum.org/agenda/2016/10/our-nuclear-facilities-are-increasingly-vulnerable-to-cyber-threats-this-is-what-policy-makers-need-to-know. See also: Ramana M. V. & Mariia Kurando (2019). Cyberattacks on Russia - the nation with the most nuclear weapons - pose a global threat. Bulletin of the Atomic Scientists, 75:1, pp.44-50.
[11] Dylevskiy I.N., Komov S.A., Petrunin A.N. On information aspects of the international legal definition of "aggression". Voennaya Mysl', 2013, №10, pp. 3-12.
[12] Alexander Fedorov and Vitaly Tsygichko, Editors. Information challenges to national and international security. M.: PIR Center, 2001. p.93

[13] Alexander Fedorov and Vitaly Tsygichko, Editors. Information challenges to national and international security. M.: PIR Center, 2001. p.122-123
[14] https://www.france24.com/en/20181107-kremlin-says-it-sees-no-prospects-better-russia-us-ties
[15] https://docs.house.gov/meetings/IF/IF00/20180411/108090/HHRG-115-IF00-Wstate-ZuckerbergM-20180411.pdf
[16] https://sg.news.yahoo.com/facebook-launches-war-room-combat-manipulation-102916292.html
[17] Justin Lynch. In rare speech, MI6 chief says cyber brings 'potentially existential challenge'. Fifth Domain. December 4, 2018.https://www.fifthdomain.com/international/2018/12/04/in-rare-speech-mi6-chief-says-cyber-brings-potentially-existential-challenge/
[18] Even though Russia and China coordinate their international approaches on international information security, for the time being each of the two mostly plays its own game, trying at least "not to shoot friendlies".
[19] Jonathan Reiber. What Happens When the US Starts to 'Defend Forward' in Cyberspace? *Defense One. November 5, 2018.* https://www.defenseone.com/ideas/2018/11/what-happens-when-us-starts-defend-forward-cyberspace/152580/
[20] Speech by Sergey Naryshkin, Director of the Foreign Intelligence Service of the Russian Federation at the Moscow Conference on International Security, April 4, 2018 http://mil.ru/mcis/news/more.htm?id=12170190@cmsArticle
[21] Elena Chernenko, Ekaterina Mareeva headlined "Cybertrophied consciousness. USA fears cyberattacks but refuses to fight them together with Russia". Kommersant, August 9, 2018.
[22] Preventing Global Nuclear Escalation and Strengthening Nuclear Security through Russian-US Dialogue. Final Report. December 29, 2018. P.7. http://www.pircenter.org/media/content/files/14/15516906100.pdf
[23] António Guterres. United Nations Secretary-General. "Securing our common future". An Agenda for Disarmament. Geneva, May 24, 2018.
[24] Preventing Global Nuclear Escalation and Strengthening Nuclear Security through Russian-US Dialogue. Final Report. December 29, 2018. P.7. http://www.pircenter.org/media/content/files/14/15516906100.pdf
[25] Definitions matter! Two decades ago, Russia proposed an agenda on "international information security". Many didn't take to that term back at the time, preferring the shorter and snappier "cybersecurity". I am aware of the fact that this is still much the case. But looking back, and in view of the threats we are facing today, it's clear that our search for global solutions should be based on the more comprehensive approach to international information security.